ÖGER Research Paper Series

Nr. 6/2024

„Künstliche Intelligenz & Online Werbung – eine datenschutzrechtliche Analyse“

verfasst von
Alexander Seyfried

Wien, 2024

https://oeger.eu/research-paper-series/

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA	andere Ansicht
ABl	Amtsblatt der EU
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der EU
AGB	Allgemeine Geschäftsbedingungen
AMS	Arbeitsmarktservice
API	Application Programming Interface („Programmierschnittstelle“)
Art	Artikel
AVV	Auftragsverarbeitungsvereinbarung
B2B	Business to Business
B2C	Business to Consumer
BCR	Binding Corporate Rules („verbindliche interne Datenschutzregeln“)
BGBl	Bundesgesetzblatt
BKartA	Bundeskartellamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw	beispielsweise
BVwG	Bundesverwaltungsgericht
bzgl	bezüglich
bzw	beziehungsweise
DA	Data Act („Daten-VO“)
DGA	Data Governance Act („Daten-Governance-VO“)
dh	das heißt
DMA	Digital Markets Act („Gesetz über digitale Märkte“)
DSA	Digital Services Act („Gesetz über digitale Dienste“)
DSB	Datenschutzbehörde(n)
DSBA	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSFA-V	Datenschutz-Folgenabschätzung-VO („Blacklist“)
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz

dt	deutsch(e)
ECG	E-Commerce-Gesetz
E-Commerce-RL	RL über den elektronischen Geschäftsverkehr
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EK	Europäische Kommission
EP	Europäisches Parlament
ePrivacy-RL	Datenschutz-RL für elektronische Kommunikation
ErwGr	Erwägungsgrund
EU	Europäische Union
EuG	Europäisches Gericht
EuGH	Europäischer Gerichtshof
evtl	eventuell(en)
f	folgend
ff	fortfolgend
Fn	Fußnote
GA	Generalanwalt
gem	gemäß
GPAI	General Purpose AI („KI-Modell mit allgemeinem Verwendungszweck“)
GPT	Generative Pre-Trained Transformer
GRC	Charta der Grundrechte der EU
grds	grundsätzlich
Hrsg	Herausgeber
idF	in der Fassung
idR	in der Regel
inkl	inklusive
insb	insbesondere
IoT	Internet of Things („Internet der Dinge“)
iSd	im Sinne des/der
iSe	im Sinne einer/eines
iSv	im Sinne von
iVm	in Verbindung mit

iZm	im Zusammenhang mit
Kap	Kapitel
KI	Künstliche Intelligenz („Artificial Intelligence: AI“)
KI-VO	KI-Verordnung („Gesetz über künstliche Intelligenz: AI Act“)
KommAustria	Kommunikationsbehörde Austria
krit	kritisch
lit	litera („Buchstabe“)
LLM	Large Language Model(s)
max	maximal
mE	meines Erachtens
mind	mindestens
Mio	Millionen
MoU	Memorandum of Understanding
MS	Mitgliedstaat(en)
Nr	Nummer
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
P2B	Plattform to Business
P2B-VO	Plattform to Business-VO
Rat	Rat der Europäischen Union
RL	Richtlinie
Rs	Rechtssache
Rsp	Rechtsprechung
RTR	Rundfunk und Telekom Regulierungs-GmbH
Rz	Randziffer
SA	Schlussanträge
SCC	Standard Contractual Clauses („Standardvertragsklauseln“)
sog	sogenannt(es)
TIA	Transfer Impact Assessment
TKG	Telekommunikationsgesetz
tlw	teilweise
TOM	Technische und Organisatorische Maßnahme(n)

ua	unter anderem
UAbs	Unterabsatz
UGP-RL	Unlautere Geschäftspraktiken-RL
UrhG	Urheberrechtsgesetz
USA	United States of America („Vereinigte Staaten von Amerika“)
usw	und so weiter
uU	unter Umständen
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
va	vor allem
verb	verbunden(e)
vgl	vergleiche
VLOP	Very Large Online Plattform („Sehr große Online-Plattform“)
VLOSE	Very Large Online Search Engine („Sehr große Online-Suchmaschine“)
VO	Verordnung
VVT	Verzeichnis der Verarbeitungstätigkeiten
VwGH	Verwaltungsgerichtshof
Z	Ziffer
zB	zum Beispiel

1 Einleitung

„*Daten sind das Gold des 21. Jahrhunderts*“.[1] Treffender kann man das Phänomen von Daten als wertvollen Rohstoff in der modernen Wirtschaft und Gesellschaft nicht beschreiben. Gerade im Bereich der (digitalen) Werbung haben Informationen aus unterschiedlichsten Quellen eine immense Bedeutung für Unternehmen, fundierte Entscheidungen zu treffen, neue Geschäftsmodelle zu entwickeln, Effizienz zu steigern und Wettbewerbsvorteile zu erlangen.[2] In immer mehr Betrieben werden dafür auch KI-basierte Anwendungen eingesetzt, denn die Verschiebung von Werbegeldern in Richtung Online-Medien nimmt stetig zu, während traditionelle Kommunikationsmittel an Bedeutung verlieren.[3] Durch das Sammeln – insb mittels „*Webcrawling*“ und „*Webscraping*“[4] – und die Analyse immer größerer Datenmengen („*Big Data*“)[5] können die Akteure Einblicke das Verhalten ihrer Kunden gewinnen, personalisierte Produkte und Dienstleistungen anbieten und ihre Marketing- und Vertriebsstrategien im Rahmen ihres Customer Relationship Managements („*CRM*“) optimieren.[6] Die Kundenzufriedenheit und Kundenbindung („*Churn Management*“)[7] sollen erhöht sowie effiziente Werbekampagnen durch KI-gesteuerte Kundensegmentierung verbessert werden.[8]

Mit dem Ziel, die Individualisierung zu automatisieren, greifen Werbetreibende oft auf „*maschinelles Lernen*“[9] bzw „*Deep Learning*“[10] zurück, welche an sich (bloße) Teilgebiete vom allumfassenden Begriff der KI sind.[11] Diese Algorithmen[12] ermöglichen eine kontinuierliche Vorhersage und Prüfung effektiver Überzeugungsstrategien, die auf den Einzelnen zugeschnitten sind („*Predictive Analytics*“).[13] Die Identifizierung von Mustern und Zusammenhängen, auch

---

1 *Judt/Klausegger*, Was ist eigentlich …Marketing 4.0? ÖBA 2022, 677 (677).
2 *Reinecke*, Datenschatz und Geschäftsmodell-Disruption: Worin liegt das strategische Potential von KI wirklich? LogR 2024, 3 (3).
3 *Maiworm* in *Chibanguza/Kuß/Steege* (Hrsg), Künstliche Intelligenz (2022) § 11 E Rz 1.
4 *Bomhard*, Text und Data Mining auf Grundlage von Webcrawling und Webscraping, InTeR 2023, 174 (174).
5 *Judt/Klausegger*, Was sind eigentlich ...Big Data? ÖBA 2019, 432 (432).
6 *Baumüller*, Big Data, SWK 23-24/2017, 1064 (1065).
7 *Oehler*, Predictive Analytics, CFO aktuell 2018, 25 (26).
8 *Krohn-Grimberghe/Nemeth/Molin*, Die Digitalisierung des CFO, CFO aktuell 2016, 21 (21).
9 *Yuan/Szypulka* in *Ebers* (Hrsg), StichwortKommentar Legal Tech (2023) Rz 1 ff, 20 ff.
10 *Gertz/Aumiller*, Legal Tech und Deep Learning - Eine Bestandsaufnahme, LTZ 2022, 30 (30).
11 *Russel/Norvig*, Künstliche Intelligenz[4] (2023) 22, 49.
12 *Sedgewick/Wayne*, Algorithmen[4] (2014) 20 ff.
13 *Luketina/Mathy/Staudingeri/Schütz/Stadlbauer/Kuci*, Predictive Analytics in der öffentlichen Verwaltung, ZTR 2021, 150 (150).

bekannt als „*Data Mining*“,[14] kann datenschutzrechtlich relevante Aspekte iSd DSGVO[15] beinhalten. Primär handelt es sich bei der automatisierten Datenanalyse nämlich um eine Verarbeitung iSd Art 4 Z 2 DSGVO.[16] Das trifft besonders dann zu, wenn die erzielten Ergebnisse Rückschlüsse über Individuen ermöglichen. Dabei ist es unerheblich, ob die zu analysierenden Daten grds anonym sind bzw vor dem Verarbeitungsvorgang durch die KI anonymisiert wurden.[17] KI-Systeme zeichnet häufig aus, dass sie die Fähigkeit besitzen, den Personenbezug (mittelbar) wiederherzustellen oder zu erzeugen, indem sie mehrere Kennzahlen und Indikatoren miteinander verknüpfen.[18] Dies auch aus aggregierten Datengruppen,[19] welche idR durch die Herstellung von „*K-Anonymität*“ in Kombination mit dem „*Differential Privacy*“-Ansatz gebildet werden.

Wie *Pieper*[20] schon festhielt, „*kann das Marketing vielleicht am meisten von KI-Anwendungen profitieren. Die Kernaktivitäten des Marketings bestehen darin, Kundenbedürfnisse zu verstehen, sie mit Produkten und Dienstleistungen in Einklang zu bringen und Menschen zum Kauf zu bewegen.*“ Dies wird durch „*Programmatic Advertising*“[21] verstärkt, bei dem einzelne Werbemöglichkeiten automatisiert und in Echtzeit gesteuert werden,[22] und verdeutlicht sich im

---

14 *Burgstaller/Hermann/Lampesberger*, Künstliche Intelligenz (2019) 80 f; vgl nunmehr auch die Definition von „Text und Data Mining“ in Art 2 Z 2 DSM-RL (EU) 2019/790, ABl 2019/L 130, 92.

15 VO (EU) 2016/679, ABl 2016/L 119, 1.

16 *Jahnel* in *Jahnel/Mader/Staudegger* (Hrsg), IT-Recht[4] (2020) Rz 10/15: Die DSGVO ist technologieneutral (vgl ErwGr 15 DSGVO).

17 Gem ErwGr 26 DSGVO gilt die DSGVO nicht für jene Informationen, deren Personenbezug entfernt wurde und die Person nicht oder nicht mehr identifiziert werden kann („*Anonymisierung*“); vgl EuGH 19.10.2016, C-582/14 (*Breyer*) Rz 46: Eine Anonymisierung liegt nur dann vor, wenn eine Re-Identifizierbarkeit der natürlichen Person nicht oder nur unter unverhältnismäßigem Aufwand nach dem derzeitigen Stand der Technik möglich wäre. Kann der Personenbezug dagegen (indirekt) wiederhergestellt werden bzw ist dies unter verhältnismäßigem Aufwand (bei Dritten) möglich, liegt nur eine „*Pseudonymisierung*“ vor, welche jedenfalls unter den Anwendungsbereich der DSGVO fällt; vgl EuG 26.4.2023, T-557/20 (*Single Resolution Board*) Rz 93: Das Gericht folgt der Ansicht des EuGH.

18 Nur 15 demografische Merkmale würden 99,98 % aller Personen einer amerikanischen Großstadt einzigartig machen. Doch reichen bereits oftmals wenige Attribute, um von einer sehr hohen Wahrscheinlichkeit einer korrekten Re-Identifizierung auszugehen. Wurden zB der Name, die Sozialversicherungsnummer und die Adresse einer Person entfernt, blieben aber das Geburtsdatum, das Geschlecht und die Postleitzahl erhalten, konnten schon im Jahr 2000 87 % der US-Bevölkerung eindeutig re-identifiziert werden. Dieses Phänomen wird fast 25 Jahre später durch den KI-Einsatz geradezu erleichtert; vgl *Rocher/Hendrickx/de Montjoye*, Estimating the success of re-identifications in incomplete datasets using generative models, nature communications (2019) 5, abrufbar unter <https://www.nature.com/articles/s41467-019-10933-3> (11.4. 2024).

19 *Heiler/Ciarnau*, Datenanonymisierung, ecolex 2022/114, 166 (166).

20 *Pieper* in *Lucas/Schuster* (Hrsg), Innovatives und digitales Marketing in der Praxis (2023) 221.

21 *Flamme/Mehlan*, Das Phänomen der politischen Online-Werbung im Zeitalter der Digitalisierung, KuR 2022, 571 (571).

22 *Prange*, Datenschutz- und lauterkeitsrechtliche Kernfragen des Einsatzes Künstlicher Intelligenz im Marketing, WRP 2024, 151 (Rz 10 ff).

Bereich der E-Mail-Werbung: So passt Cosabella, ein Einzelhändler für Luxusdessous, mithilfe seiner KI jede Nachricht individuell an die Reaktionen seiner Kunden auf vorherige E-Mails, ihre getätigten Umsätze und ihre Interessen an. Bspw werden jene Konsumenten, die wenig Geld ausgeben oder inaktiv sind, gezielt mit einer E-Mail über einen Happy Hour-Verkauf informiert, bei dem sie während eines bestimmten Zeitraums einen Rabatt in Höhe von 20 % erhalten können. Hingegen erhalten Kunden, die regelmäßig viel Geld ausgeben, keine Rabattaktionen, sondern gezielte Werbeangebote für neue Modelle.[23]

Aus diesen Gründen gibt es Bedenken, dass bestehende Vertragsmechanismen[24] umgangen werden, wenn Verträge von selbstlernenden KI-Programmen abgeschlossen und durchgeführt werden,[25] ohne dass den Beteiligten klar ist, welche Verpflichtungen damit einhergehen und warum.[26] Im Gegenteil, es ist va diese – und in Zukunft noch intensiver hervorkommende – „*selbstständige Entscheidungsfindung*“,[27] die KI auszeichnet. Immer öfter wird KI verwendet, um positive Bewertungen von erfundenen Personen zu generieren, die für gefälschte Produkt- oder Dienstleistungsbewertungen eingesetzt werden. Dass KI-Systeme ferner in der Lage sind, Gesichtsreaktionen, Emotionen und Sprachmuster zu erkennen,[28] ist längst auch im CRM Realität[29] und wird als „*Affective Computing*“[30] bezeichnet. Ende März 2024 enthüllte OpenAI (ua der Entwickler von ChatGPT) die sog „*Voice Engine*“, mit welcher fortan Stimmen imitiert werden können.[31] Dies alles abseits geläufiger (unlauterer) Werbetricks wie „*Nudging*“,[32]

---

[23] eTail25, How Cosabella Is Using AI to Boost Sales with Email, abrufbar unter <https://etaileast.wbresearch.com/blog/how-cosabella-uses-ai-to-boost-sales-with-email> (19.4.2024).

[24] *Haidinger/Hufnagl* in *Hanzl/Pelzmann/Schragl* (Hrsg), Handbuch Digitalisierung (2021) 497 ff.

[25] *Tercero* in *Raffling/Schock* (Hrsg), Digitale Wirtschaft und Industrie 4.0 (2018) 7 ff.

[26] *Rabl* in *Felten/Kofler/Mayrhofer/Perner/Tumpel* (Hrsg), Digitale Transformation im Wirtschafts- & Steuer recht (2019) 32 (Rz 2/13).

[27] *Dablander*, Künstliche Intelligenz und Datenökonomie (Stand 22.3.2024, Lexis Briefings in lexis360.at).

[28] *Caldarola/Schrey* in *Caldarola/Schrey* (Hrsg), Big Data und Recht (2019) H VI Rz 329.

[29] EDSA 20.5.2022, Data protection issues arising in connection with the use of Artificial Intelligence, abrufbar unter <https://www.edpb.europa.eu/news/national-news/2022/data-protection-issues-arising-connection-use-artificial-intelligence_de> (11.4.2024): Telefongespräche eines Kundendienstes werden aufgezeichnet. Jede Nacht analysiert die KI-Software automatisch alle neuen Audioaufzeichnungen nach Schlüsselwörtern und eruiert den emotionalen Zustand des Kunden zum Zeitpunkt des Anrufs. Es wird eine Liste erstellt, welche die Betroffenen nach der Wahrscheinlichkeit ihrer Unzufriedenheit sortiert. Mitarbeiter rufen die auf diese Weise ausgeforschten Kunden im Anschluss an, um die Gründe ihrer Unzufriedenheit in Erfahrung zu bringen.

[30] *Hoffmann-Riem*, Die digitale Transformation als rechtliche Herausforderung, JuS 2023, 617 (625).

[31] OpenAI 29.3.2024, Navigating the Challenges and Opportunities of Synthetic Voices, abrufbar unter <https://openai.com/blog/navigating-the-challenges-and-opportunities-of-synthetic-voices> (12.4.2024): OpenAI ist sich der Herausforderungen seines Systems bewusst und hat daher beschlossen, dieses vorerst – aufgrund von Sicherheits- und insb Missbrauchsbedenken – nicht zu veröffentlichen.

[32] *Judt/Klausegger*, Was ist eigentlich ... Nudging? ÖBA 2020, 416 (416).

„*Deepfakes*“[33] oder „*Dark Patterns*“.[34] Der EuGH[35] betont völlig zu Recht die Notwendigkeit besonderer Verfahrensgarantien, wenn automatisierte Entscheidungen (hier: Uploadfilter) in grundrechtssensiblen Bereichen getroffen werden.

Vor diesem Hintergrund ist ua der künftige ErwGr 29 KI-VO[36] zu messen, wonach „*übliche und rechtmäßige Geschäftspraktiken, bspw im Bereich der Werbung, die im Einklang mit den geltenden Rechtsvorschriften stehen, als solche nicht als schädliche manipulative KI-Praktiken gelten [sollten]*“, obwohl im selben ErwGr ausdrücklich steht, dass „*KI-gestützte manipulative Techniken dazu verwendet werden [können], Personen zu unerwünschten Verhaltensweisen zu bewegen oder sie zu täuschen, indem sie in einer Weise zu Entscheidungen angeregt werden, die ihre Autonomie, Entscheidungsfindung und freie Auswahl untergraben und beeinträchtigen.*“ Es stellt sich die Frage, ob und wann die Schwelle einer solchen Verhaltensmanipulation überschritten wird, sodass personalisierte Werbung oder andere Formen von Marketingmaßnahmen als verboten (Art 5 KI-VO), hochriskant (Art 6 ff KI-VO) oder doch nur als wenig risikoreich zu qualifizieren sind.

In dieser Arbeit soll daher untersucht und dargestellt werden, (i) welche datenschutzrechtlichen Herausforderungen sich bereits vor der KI-VO durch den Einsatz von KI-Systemen in der Online-Werbung ergaben, (ii) ob die KI-VO als effektive Lösung für gegenwärtige und zukünftige Probleme angesehen werden kann oder ob bestimmte Risiken im Bereich des Marketings evtl nicht vollständig angesprochen oder vernachlässigt wurden, und (iii) welche Rolle der DSGVO in diesem Zusammenhang zukommt.

Der Hauptfokus dieser Arbeit liegt auf dem Datenschutzrecht und seiner Interaktion mit der KI-VO im Kontext von KI-unterstützten und KI-autonomen Werbemaßnahmen. Unlautere (ua aggressive und irreführende Geschäftspraktiken) sowie sonstige wettbewerbs- und

---

33 *Kumkar/Rapp*, Deepfakes, ZfDR 2022, 199 (200 ff).

34 *Schneider*, Dark Patterns, DSB 2023, 222 (222).

35 EuGH 26.4.2022, C-401/19 (*Polen/EP und Rat*) Rz 24, 40 f, 98.

36 EP 13.3.2024, P9_TA(2024)0138, abrufbar unter <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html> (11.4.2024), zuletzt geändert durch EP 17.4.2024, cor01, abrufbar unter <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf> (19.4.2024): Es wurden bloß Änderungen in der Sprache und Nummerierung vorgenommen. Die vorliegende Arbeit stützt sich auf die Version der KI-VO, die vom EP in erster Lesung angenommen wurde und den ursprünglichen Entwurf der EK vom 21.4.2021, COM(2021) 206 final, als Ergebnis der Trilogverhandlungen ersetzt. Eine formale Zustimmung des Rates und die Veröffentlichung im EU-Amtsblatt stehen noch aus.

verbraucherschutzrechtliche Aspekte werden grds nicht behandelt. Es kann jedoch vorkommen, dass in bestimmten Teilen dieser Abhandlung darauf Bezug genommen wird, weil das Online-Marketing – sowie KI per se – als Querschnittsmaterie viele Teilgebiete der Rechtswissenschaften berührt. Nichtsdestotrotz wird das Urheberrecht vollständig ausgeklammert. Auch andere Immaterialgüterrechte wie das Marken- und Patentrecht sowie die Bedeutung von KI-Systemen im arbeitsrechtlichen Umfeld (zB der Einsatz von KI zur Überwachung von Arbeitnehmern) werden nicht näher erläutert. Es sei darauf hingewiesen, dass vereinzelt auf die neue europäische Plattformregulierung (insb DMA[37] und DSA[38]) und Datenregulierung (insb DA[39] und DGA[40]) eingegangen wird.

Der Verlauf der Untersuchung gestaltet sich wie folgt: Im zweiten Kapitel wird eine grundlegende Einführung in die gegenwärtigen Unsicherheiten gegeben, die sich in der Werbung aus datenschutzrechtlicher Perspektive ergeben. Es wird darauf hingewiesen, dass bestimmte Praktiken seit Inkrafttreten der DSGVO – selbst ohne den Einsatz von KI-Systemen – vermehrt Gegenstand von Diskussionen und Streitigkeiten waren und weiterhin sind. Anschließend werden im dritten Kapitel bedeutende Bestimmungen der KI-VO im werberechtlichen Kontext einzeln behandelt und kritisch analysiert. Es werden die Erkenntnisse des zweiten Kapitels auf die KI-VO übertragen sowie die besprochenen Herausforderungen diesem neuen Regelwerk zugeordnet. Abschließend wird noch kurz das Verhältnis zwischen der KI-VO und der DSGVO beleuchtet.

Begriffsdefinitionen und weitere Anmerkungen, die für das Verständnis der vorliegenden Untersuchung als wesentlich erachtet werden, aber den Lesefluss selbst nicht stören sollen, finden sich in den entsprechenden Fußnoten wieder.

[37] VO (EU) 2022/1925, ABl 2022/L 265, 1.
[38] VO (EU) 2022/2065, ABl 2022/L 277, 1.
[39] VO (EU) 2023/2854, ABl 2023/Reihe L, 1.
[40] VO (EU) 2022/868, ABl 2022/L 152, 1.

2 Aktuelle datenschutzrechtliche Herausforderungen iZm KI & Online-Werbung

2.1 Tracking & Cookies

Schon bisher können Werbetreibende ihre Zielgruppen im Zuge der Datenverarbeitung genau identifizieren[41] und Werbebotschaften exakt an diese ausrichten („*Targeted Advertising*“).[42] Sie erkennen (zukünftige) Verhaltensmuster und Trends, insb über die Klickrate,[43] und passen Anzeigeninhalte in Echtzeit an individuelle Bedürfnisse und demografische Merkmale (zB Geschlecht, Alter und sozialer Status) an.[44] Das prominenteste Beispiel solcher Tracking-Methoden sind „*Cookies*“.[45] Dabei erfordert der Einsatz von technisch nicht-notwendigen[46] Cookies zu Analyse- und Werbezwecken eine ausdrückliche, freiwillige und aktive Einwilligung des Nutzers für den jeweils konkreten Fall[47] auf Basis klarer und umfassender Informationen iSd Art 4 Z 11 iVm Art 7 DSGVO.[48] Dies hat nicht zuletzt der EuGH[49] klargestellt, wonach vorab angekreuzte Kontrollkästchen unzulässig sind (vgl auch ErwGr 32 DSGVO).[50] Anstelle eines bloßen Opt-Out[51] wird vielmehr ein explizites Opt-In[52] verlangt. Daher ist zB ein Cookie für verhaltensbasierte Werbung nicht technisch erforderlich, selbst wenn er die einzige Einnahmequelle einer Webseite darstellt und deren Betrieb von diesen Einnahmen abhängt. Ebenso können Analyse-Cookies, wie etwa zur Besucherzählung, nicht als technisch notwendig eingestuft werden, auch wenn sie aus Sicht eines Webseitenbetreibers von wirtschaftlichem Nutzen sein mögen. Solche Cookies dürfen daher nur nach vorheriger Information und Einwilligung der Nutzer gesetzt werden.[53]

---

41 *Škorjanc*, Künstliche Intelligenz im Finanzsektor) ÖBA 2023, 427 (428).

42 *Geringer/Stückler*, Daten im Bilanzsteuerrecht, ÖStZ 2020/190, 149 (149).

43 OECD 5.10.2015, Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report (2015) Rz 138, abrufbar unter <https://www.oecd.org/ctp/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report-9789264241046-en.htm> (9.5.2024).

44 *Geuer/Wollmann* in *Hanzl/Pelzmann/Schragl* (Hrsg), Handbuch Digitalisierung (2021) 613, 625 ff.

45 *Illibauer* in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020) Kap 17 Rz 17.56 ff.

46 BVwG 12.3.2019, W214 2223400-1.

47 *Thiele*, DSB: Einwilligung in Tracking- und Marketing-Cookies zulässig, ZIIR 2023, 37 (37, 45 f).

48 Vgl Art 5 Abs 3 ePrivacy-RL (2002/58/EG), ABl 2002/L 201, 37 – geändert durch Cookie-RL (2009/136/EG), ABl 2009/L 337, 11 – welcher in Österreich in § 165 Abs 3 TKG 2021, BGBl I 190/2021 idF BGBl I Nr 6/2024, umgesetzt wurde.

49 EuGH 1.10.2019, C-673/17 (*Planet49*) Rz 65, 71, 82.

50 *Thiele*, EuGH: Setzen von Cookies erfordert aktive Einwilligung des Internetnutzers, ZIIR 2019, 440 (440 ff).

51 *Bisset/Raabe-Stuppnig*, Datenschutz im Telekommunikationsrecht (Stand 22.3.2024, Lexis Briefings in lexis360.at).

52 *Kerbl*, Website und Cookies (Stand 9.4.2023, Lexis Briefings in lexis360.at).

53 *Pils*, Datenschutz im Marketing[2] (2024) 38.

Es zeigt sich, dass Unternehmen bereits seit geraumer Zeit gut beraten sind, geeignete „*Consent-Management-Tools*“[54] zu entwickeln und bereitzustellen.[55] In der Praxis hat sich mittlerweile leider ein wahrlicher Wildwuchs an unterschiedlichsten „*Cookie-Bannern*“ etabliert,[56] welche einmal mehr, einmal weniger oder überhaupt nicht rechts- bzw datenschutzkonform sind.[57]

Ebenso erfordert die Verwendung (kostenpflichtiger) Internet-Statistik-Tools, welche idR von Webshop-Betreibern eingesetzt werden, die Zustimmung der Besucher des jeweiligen Webshops.[58] Durch den Einsatz derartiger Hilfsmittel können Unternehmen ua verwertbare Informationen über die Anzahl der Seitenaufrufe, die Verweildauer, die geografische Herkunft und die Anzahl der getätigten Bestellungen einzelner Besucher erhalten. Darüber hinaus können sie Kenntnisse über durchgeführte oder unterlassene Anmeldungen, Registrierungen sowie Klicks auf Anzeigen gewinnen.[59] Erfahrungsgemäß ist es va Google Analytics, das eine ausgiebigere Webanalyse anbietet und gründliche Benutzerprofile im Zuge der Datenverarbeitung anlegt.[60] Die DSB[61] steht dem Einsatz von Google Analytics mehr als kritisch gegenüber und stellte fest, dass auch anonymisierte IP-Adressen[62] zum digitalen Fußabdruck gehören, die eine Person bei Dritten (hier: Google) identifizierbar machen.[63]

---

54 *Stadler/Bauer/Chochola* in *Bichler* (Hrsg), Praxishandbuch Marketingrecht (2024) 323 ff.

55 Vgl EDSA 4.5.2020, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679$^{v1.1}$, Rz 6 ff, abrufbar unter <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf> (9. 5.2024); DSB, Fragen und Antworten, Analytics & Cookies, abrufbar unter <https://www.dsb.gv.at/download-links/fragen-und-antworten.html#Analytics&Cookies> (5.4.2024); DSB, FAQ zum Thema Cookies und Datenschutz (Stand 20.12.2023), abrufbar unter <https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html> (5.4.2024).

56 *Ettig*, Warten auf Godot - Noch immer keine Neuregelung für Cookies & Co., KuR 2024 H 4, I (I).

57 *Pollirer*, Checkliste datenschutzgerechte Cookie-Banner, Dako 2022/18, 38 (38).

58 *Mayer*, Webshop-Recht^{2} (2019) 164.

59 *Lachenmann* in *Koreng/Lachenmann* (Hrsg), Formularhandbuch Datenschutzrecht^{3} (2021) F I 5 Anm 1-10.

60 *Schröder* in *Schröder* (Hrsg), Datenschutzrecht für die Praxis^{5} (2023) 185 ff.

61 DSB 22.4.2022, D155.026 (2022-0.298.191) (*Google Analytics II*); *Messner/Mosing*, ÖDSB: Datenübermittlung durch Implementierung von Google Analytics, ZD 2022, 493 (495 ff).

62 DSB 22.12.2021, D155.027 (2021-0.586.257) (*Google Analytics I*): Nicht-anonymisierte IP-Adressen können zur Identifizierbarkeit der natürlichen Person führen; vgl *Schweiger*, Google Analytics: Der nicht rechtskräftige Teilbescheid der DSB, DSB 2022, 52 (52).

63 *Böszörmenyi*, Google Analytics - kein Risiko, dennoch verboten? ecolex 2023, 164 (164).

Weiters hielt der EuGH[64] erst kürzlich fest, dass sogar der aus einem Consent Management Portal („*CMP*“) gewonnene codierte Transparency-and-Consent String („*TC-String*“)[65] ein personenbezogenes Datum ist, weil die natürliche Person über ein Cookie der IP-Adresse im CMP mittelbar identifiziert werden kann, selbst wenn nicht alle (hier: gemeinsamen) Verantwortlichen eine Zugriffsmöglichkeit auf dieses Cookie haben.[66] Die konkreten Auswirkungen dieses Urteils auf die Werbebranche lassen sich noch nicht gänzlich abschätzen, insb weil sich der EuGH bedauerlicherweise nicht zur Rechtmäßigkeit der Vorgehensweise der IAB Europe iZm dem sog Real Time Bidding („*RTB*“)[67] insgesamt äußerte.[68] Abzuwarten bleibt auch, inwiefern diese Entscheidung die Tätigkeit sog „*Datenvermittlungsdienste*“ iSd Art 2 Z 11 DGA beeinflussen wird, welche die Verwertung personenbezogener Daten unter gewissen Voraussetzungen vornehmen können (Art 10 ff DGA iVm ErwGr 27 ff DGA).[69] Dabei ist ua auf eine Konformität mit der DSGVO zu achten (Art 1 Abs 3 DGA iVm ErwGr 4, 35 DGA).

Ungeachtet dessen und unter der Voraussetzung, dass die Möglichkeit des jederzeitigen Widerspruchs (Art 21 DSGVO) besteht, mag es für Unternehmen im Bereich der Direktwerbung[70] zulässig sein, die strengen Anforderungen an eine Einwilligung zu umgehen, indem sie sich auf

---

64 EuGH 7.3.2024, C-604/22 (*IAB Europe*) Rz 20 ff, 51.

65 Dieser enthält wesentliche Informationen iZm der Einwilligung des Nutzers (zB worin er eingewilligt und wogegen er Widerspruch eingelegt hat) in codierter Form (Kombination aus Buchstaben und Zeichen), welcher mit Werbetreibenden, Werbeplattformen und Datenbrokern geteilt wird, damit diese personalisierte Werbung schalten können. Durch die Kombination vom TC-String und der IP-Adresse, die über ein Cookie am Gerät des Nutzers ausgelesen wird, ist die Codierung obsolet und der Nutzer eindeutig identifizierbar; vgl *Kriwanek/Tuma*, EuGH: Datenschutz – Datencodierung iZm personalisierter Werbung (14.03.2024, LexisNexis Rechtsnews 35185 in lexis360.at).

66 *Herbrich*, Personalisierte Online-Werbung, ZD-Aktuell 2024, 01623 (beck-online).

67 RTB ist ein automatisierter Prozess, der es Werbetreibenden ermöglicht, Anzeigenplatzierungen in Echtzeit zu kaufen und zu verkaufen. Hierbei werden Anzeigenplätze auf Websites oder in mobilen Apps in Auktionen verfügbar gemacht, die in Bruchteilen von Sekunden stattfinden, wenn eine Webseite oder App geladen wird. Werbetreibende bieten dann in Echtzeit auf diese Anzeigenplätze, basierend auf Informationen über den Nutzer und den Wert der Platzierung für ihre Kampagne. Die Auktion erfolgt oft über spezialisierte Plattformen, die als „*Ad Exchanges*“ bekannt sind. Der Bieter mit dem höchsten Gebot gewinnt die Auktion und seine Anzeige wird sofort auf der Website oder in der App angezeigt. RTB ermöglicht es Unternehmen, ihre Anzeigen gezielt an relevante Zielgruppen auszuspielen und die Effizienz ihrer Kampagnen in Echtzeit zu optimieren. Zu Datenschutzverstößen kommt es, wenn keine Zustimmung der Betroffenen vorliegt; vgl auch *Baumgartner/Hansch*, Onlinewerbung und Real-Time-Bidding, ZD 2020, 435 (435); *Greiner*, Guidelines für den Einsatz von Real-Time Bidding, ecolex 2020, 172 (172).

68 *Vasella* 12.3.2024, EuGH i.S. IAB Europe: weite Auslegung des Begriffs des Personendatums: Verbindung aufgrund des Zwecks reicht; gemeinsame Verantwortung von IAB mit den Mitgliedern, abrufbar unter <https://datenrecht.ch/eugh-i-s-iab-europe-weite-auslegung-des-begriffs-des-personendatums-verbindung-aufgrund-des-zwecks-reicht-gemeinsame-verantwortung-von-iab -mit-den-mitgliedern> (10.4.2023).

69 *Fischer*, Die Datenverwertungsgesellschaft, ÖBl 2023/44, 148 (148).

70 *Mertens*, OLG Stuttgart: Direktwerbung und Adresshandel können berechtigte Interessen darstellen, DSB 2024, 104 (104).

ihr berechtigtes Interesse gem Art 6 Abs 1 lit f DSGVO berufen.[71] Jedoch sind das Tracking und die anschließende automatisierte Profilerstellung[72] idR derart eingriffsintensiv,[73] dass das Interesse der betroffenen Personen an der Achtung ihrer Privatsphäre und dem Schutz ihrer personenbezogenen Daten im Einzelfall sehr häufig überwiegen werden.[74] Die obligatorische Interessenabwägung durch den datenschutzrechtlich Verantwortlichen müsste diesfalls wohldurchdacht und sehr gut dokumentiert worden sein.

Es bleibt spannend abzuwarten, ob der Einsatz von KI möglicherweise dazu führen wird, dass die Verwendung von Cookies überflüssig wird. Es könnte sein, dass fortschrittliche KI-Technologien in der Lage sind, das Verhalten von Nutzern so präzise zu analysieren und Vorlieben so genau vorherzusagen, dass traditionelle Methoden wie Cookies weniger relevant werden. Dies könnte eine Entwicklung hin zu neuen – evtl noch invasiveren – Ansätzen im Bereich der Datenerfassung und Analyse bedeuten.

2.2 Drittstaatenproblematik (am Beispiel von ChatGPT)

Das Dilemma eines Drittstaatenbezugs ergibt sich seit *Schrems I*[75] und *Schrems II*[76] vorrangig aus einem unzulässigen Datentransfer in die USA. Auch der Angemessenheitsbeschluss der EK[77] für das nunmehrige „*EU-US Data Privacy Framework*“[78] bietet diesbezüglich wohl keine geeignete Rechtsgrundlage iSd Art 45 DSGVO für eine rechtmäßige Übermittlung personenbezogener Daten in die USA. Einerseits ist bereits eine erste Nichtigkeitsklage beim EuG anhängig,[79] andererseits hat Maximilian Schrems bzw dessen Datenschutz-Verein Noyb verlautbart, gegen diesen gerichtlich vorgehen zu wollen.[80] Unternehmen sollten sich daher bewusst

[71] Vgl auch § 174 TKG 2021.
[72] Vgl Kapitel 2.7 (Profiling).
[73] *Gausling*, Künstliche Intelligenz im digitalen Marketing, ZD 2019, 335 (338 f).
[74] DSK 20.12.2021, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien, 31, abrufbar unter<https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf>(20.4.2024).
[75] EuGH 6.10.2015, C-362/14 (*Schrems I*) Rz 107.
[76] EuGH 16.7.2020, C-311/18 (*Schrems II*) Rz 203.
[77] EK 10.7.2023, Adequacy decision for the EU-US Data Privacy Framework, C(2023) 4745 final, abrufbar unter <https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en> (10.4.2024).
[78] *Kern*, Das neue EU-US Data Privacy Framework als Rechtsgrundlage für Datentransfers in die USA, ecolex 2023, 982 (982).
[79] EuG laufend, T-553/23 (*Latombe*); vgl EuG 12.10.2023, T-553/23 R (*Latombe*): Das Gericht wies den Antrag auf Gewährung vorläufigen Rechtsschutzes mangels Dringlichkeit ab.
[80] Noyb 10.7.2023, European Commission gives EU-US data transfers third round at CJEU, abrufbar unter <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> (5.4.2024).

sein, dass ein gewisses Risiko besteht, wenn sie ihre Datentransfers auf Art 45 DSGVO stützen. Mittelfristig gesehen könnte der Angemessenheitsbeschluss wegfallen, weshalb es ratsam wäre, bereits jetzt über alternative Lösungen zur Legitimation von Übertragungen in die USA nachzudenken. Angemerkt wird, dass die Kritik am neuen Abkommen durchaus berechtigt ist, denn die faktischen Eingriffsmöglichkeiten der US-Behörden sind nach wie vor existent.[81] Erst vor kurzem votierte der US-Kongress dafür, den umstrittenen Foreign Intelligence Surveillance Act („*FISA*“) zu verlängern, der es amerikanischen Behörden auch in Zukunft ermöglichen wird, ausländische Kommunikation ohne Gerichtsbeschluss zu überwachen.[82] Auch der sog „*Cloud Act*“ erlaubt es US-Behörden seit 2018, auf Kundendaten zuzugreifen, die von US-Unternehmen (zB Microsoft) in der Cloud gespeichert werden, unabhängig davon, ob sich diese Daten auf Servern innerhalb oder außerhalb der USA (zB Europa) befinden.[83] Konsequenterweise wird Ausländern (EU-Bürgern) weiterhin kein gleichwertiges Datenschutzniveau garantiert, sodass ein *Schrems III*- bzw *Latombe*-Urteil äußerst wahrscheinlich ist.[84]

Diese aus datenschutzrechtlicher Sicht prekäre Situation, welche in der Vergangenheit bspw durch Cookiebot[85] und Google Analytics[86] aufgezeigt wurde, wird gegenwärtig durch den Einsatz von KI-Modellen untermauert: Viele bekannte Anbieter sog LLM[87] – allen voran OpenAI – haben Niederlassungen in der EU (zB OpenAI in Irland). Die Mutterunternehmen haben ihren Sitz jedoch in den USA (zB OpenAI in Kalifornien). Deswegen müssen sich private sowie kommerzielle Nutzer von ChatGPT darüber im Klaren sein, dass es in jedem Fall zu einer Übertragung von personenbezogenen Daten in die USA kommt. Dies geht mE mehr oder weniger

---

81 *Denga*, Die neue transatlantische Datenordnung "Privacy-Framework" und "Privacy Shield II", RIW 2023, 625 (625).

82 TheVerge 12.4.2024, House votes to reauthorize FISA, without the warrant requirement amendment, abrufbar unter <https://www.theverge.com/2024/4/12/24128600/fisa-section-702-house-votes-to-reauthorize-warrant-requirement> (18.4.2024).

83 Conceptboard, Der US Cloud Act: Die Bedrohung des europäischen Datenschutzes, abrufbar unter <https://conceptboard.com/de/blog/us-cloud-act-europaeischer-datenschutz/> (24.6.2024).

84 *Anderl/Tlapak*, Neuer Angemessenheitsbeschluss der Kommission für Datentransfers in die USA, ecolex 2023, 796 (796).

85 *Schneider*, Cookiebot, DSB 2022, 2 (2).

86 DSB 22.12.2021, D155.027 (2021-0.586.257).

87 *Waxnegger*, Künstliche Intelligenz und Strafrecht (2024) 16.

transparent aus den AGB und Datenschutzerklärungen von OpenAI hervor,[88] welche zwischen der individuellen[89] und der geschäftlichen[90] Nutzung von ChatGPT differenzieren.[91]

Besondere Vorsicht ist daher geboten, wenn Mitarbeiter oder gar die Unternehmensführung private ChatGPT-Accounts im täglichen Büroalltag verwenden.[92] Die Angesprochenen verarbeiten – bewusst oder unbewusst – (sensible) Daten mit Personenbezug durch ihre Interaktionen und Eingaben („*Prompts*“)[93] mit ChatGPT; sei es auch nur, um Texte zusammenzufassen.[94] Dabei kann es sich um ihre eigenen[95] als auch die Daten Dritter (zB anderer Mitarbeiter, Kunden oder Geschäftspartner)[96] handeln. Es ist wichtig zu betonen, dass personenbezogene Daten (inkl Betriebs- und Geschäftsgeheimnisse)[97] grds nur mit Zustimmung der Betroffenen in ChatGPT eingegeben oder hochgeladen werden sollten, andernfalls idR keine rechtmäßige Verarbeitung vorliegt.[98]

Zum besseren Verständnis soll ein kurzer Einblick in die Datenschutzerklärung von OpenAI („*Privacy Policy*“)[99] für in der EU lebende Privatnutzer gegeben werden. Dort finden sich maßgebliche Bestimmungen unter Punkt 1 („*Verantwortlicher*“): „*Wenn Sie im Europäischen Wirtschaftsraum („EWR“) oder in der Schweiz leben, ist OpenAI Ireland Limited [...]*

88 OpenAI Policies, abrufbar unter <https://openai.com/policies> (10.4.2024).

89 „*ChatGPT for Individuals*“: Hier wird zwischen einer kostenfreien („*Free*“) und kostenpflichtigen („*Plus*“) Variante unterschieden.

90 „*ChatGPT for Businesses*“: Hier können Unternehmen ChatGPT entweder über APIs in ihr Unternehmen integrieren oder Firmenaccounts für Mitarbeiter anlegen („*Teams*“ oder „*Enterprise*“).

91 OpenAI ChatGPT Geschäftsmodelle, abrufbar unter <https://openai.com/chatgpt/pricing> (10.4.2024).

92 Dieses Problem stellt sich mE nicht bei der Nutzung privater Accounts für rein persönliche oder familiäre Zwecke, weil in solchen Fällen die Haushaltsausnahme gem Art 2 Abs 2 lit c DSGVO (ErwGr 18 DSGVO) einschlägig wird; vgl auch EuGH 10.7.2018, C-25/17 (*Jehovan todistajat*) Rz 41: Die Ausdrücke „*persönlich*“ und „*familiär*“ beziehen sich auf die Tätigkeit der Person, die personenbezogene Daten verarbeitet, und nicht auf die Person, deren Daten verarbeitet werden.

93 „*Eingabedaten*“ (Input) iSd der KI-VO sind die in ein KI-System eingespeisten oder von diesem direkt erfassten Daten, auf deren Grundlage das System eine Ausgabe (Output) hervorbringt (Art 3 Z 33 KI-VO); vgl *Busche*, Einführung in die Rechtsfragen der künstlichen Intelligenz, JA 2023, 441 (445).

94 *Gerhartl*, Der Einsatz künstlicher Intelligenz im Arbeitsrecht, ASoK 2023, 390 (390).

95 Bzgl ihrer eigenen Daten liegt die Verantwortung für die Nutzung bei den Mitarbeitern selbst.

96 *Rauer*, Künstliche Intelligenz und der Versuch einer Regulierung - Die KI-Verordnung, BB 2024 H 7, I (I).

97 Grds auch nicht in anonymisierter Form, denn es darf nicht übersehen werden, dass die Anonymisierung an sich eine Verarbeitung iSd DSGVO darstellt, die ihrerseits einer Rechtsgrundlage bedarf, welche idR nicht vom ursprünglichen Verarbeitungszweck gedeckt sein wird. Es sollte also jedenfalls schon bei Erhebung der Daten gegenüber Betroffenen offengelegt werden, dass eine Anonymisierung stattfinden kann und diese Daten anschließend entsprechend weiterverarbeitet werden können.

98 *Rohrleitner*, ChatGPT und Mitarbeiter:innen - ein Risiko? Dako 2023/43, 84 (84).

99 OpenAI Privacy Policy (Stand 15.12.2023), abrufbar unter <https://openai.com/de/policies/eu-privacy-policy> (10.4.2024); OpenAI Nutzungsbedingungen für Europa (Stand 14.11.2023), abrufbar unter <https://openai.com/de/policies/eu-terms-of-use> (11.4.2024): Diese gelten für Privatnutzer in der EU.

Verantwortlicher und ist für die Verarbeitung Ihrer personenbezogenen Daten [...] verantwortlich", sowie unter Punkt 9 („*Datenübermittlungen*"): „*Durch die Nutzung unserer Dienste verstehen Sie und erkennen Sie an, dass Ihre personenbezogenen Daten in unseren Einrichtungen und auf unseren Servern in den USA verarbeitet und gespeichert werden."* Im Ergebnis fällt damit die Verarbeitung (inkl Speicherung) der Nutzerdaten sowie aller Informationen und Dokumente, welche diese eingeben oder hochladen,[100] unter die DSGVO.[101]

Ernstzunehmen ist, dass OpenAI bis heute nicht in der vom US-Handelsministerium geführten „*Data Privacy Framework List*"[102] aufscheint. Aus diesem Grund ist mE – unabhängig davon, ob ChatGPT kommerziell oder privat genutzt wird – von keinem angemessenen Datenschutzniveau auszugehen, da aus der Datenschutzerklärung nicht klar und eindeutig hervorgeht, ob stattdessen (genehmigungsfreie) „*geeignete Garantien*"[103] bestehen, die Betroffenen durchsetzbare Rechte und effektive Rechtsbehelfe zur Verfügung stellen. In der Privacy Policy[104] findet sich lediglich der Passus, dass sich OpenAI ua „*für die Übermittlung [der] personenbezogenen Daten in Länder außerhalb des EWR [...] auf die Angemessenheitsbeschlüsse der Europäischen Kommission [...] und auf die von der Europäischen Kommission genehmigten Standardvertragsklauseln*" stützt.

Ob OpenAI tatsächlich diese SCC (Art 46 DSGVO)[105] abgeschlossen hat, ist unklar, weil das Unternehmen seiner diesbezüglichen Informationspflicht gem Art 13 Abs 1 lit f DSGVO[106] nicht ausreichend nachkommt.[107] Auf die empfehlenswerte Durchführung eines TIA soll hier nur am

[100] Vgl Punkt 2 Privacy Policy: „*Nutzerinhalte*" sind alle Eingaben und Datei-Uploads, die ein Nutzer OpenAI bzw dessen Diensten (zB ChatGPT, Sora und DALL-E) zur Verfügung stellt.

[101] Die DSGVO ist auch dann (räumlich) anwendbar, wenn die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen in der EU erfolgt, auch wenn die Verarbeitung per se in einem Drittstaat stattfindet (Art 3 Abs 1 DSGVO iVm ErwGr 22 DSGVO).

[102] U.S. Department of Commerce, Data Privacy Framework List, abrufbar unter <https://www.dataprivacyframework.gov/list> (10.4.2024).

[103] *Tichy/Leissler/Woller*, Cloud Computing (2019) Rz 303 ff.

[104] Vgl Punkt 9 Privacy Policy.

[105] *Sedef/Steiner*, Internationaler Datentransfer (Stand 21.3.2024, Lexis Briefings in lexis360.at).

[106] Als Datenexporteur müsste „*OpenAI Irland*" solche Standardvertragsklauseln (SCC) mit „*OpenAI USA*" als Datenimporteur vereinbaren und die Betroffenen darüber informieren, wo sie diese einsehen oder wie sie eine Kopie davon erhalten können. Bei der Verarbeitung personenbezogener Daten aus öffentlichen Quellen greift die korrespondierende Pflicht gem Art 14 Abs 1 lit f DSGVO.

[107] *Schmidt-Wudy* in *Wolff/Brink/von Ungern-Sternberg* (Hrsg), BeckOK Datenschutzrecht[47.EL] (2024) Art 14 Rz 56; *Illibauer* in *Knyrim* (Hrsg), DatKomm Art 13 Rz 38 (Stand 1.12.2021, rdb.at).

Rande hingewiesen werden.[108] Fraglich ist zudem, ob OpenAI interne BCR (Art 47 DSGVO)[109] angenommen hat, auf welche der Transfer alternativ gestützt werden dürfte.[110] In der Datenschutzerklärung fehlt ein entsprechender verpflichtender Hinweis. Letztlich bleiben nur die Ausnahmetatbestände des Art 49 Abs 1 UAbs 1 DSGVO,[111] um die Übermittlung in die USA zu legitimieren. Zu denken ist hierbei etwa an die explizite Einwilligung der Betroffenen (lit a) oder die Vertragserfüllung (lit b). Ob sich OpenAI als Ultima Ratio[112] auf sein zwingendes[113] berechtigtes Interesse (Art 49 Abs 1 UAbs 2 DSGVO) stützen kann, unterliegt einer besonders strengen Interessenabwägung im jeweiligen Einzelfall.[114] Weiters ist es an restriktiv auszulegende[115] kumulative Voraussetzungen geknüpft. Zwar spricht ErwGr 113 DSGVO von „*legitimen gesellschaftlichen Erwartungen in Bezug auf einen Wissenszuwachs*“,[116] doch kann sich OpenAI schon deshalb nicht auf diese Ausnahme berufen, weil (i) die „*Übermittlung nicht wiederholt erfolgen*“[117] und (ii) die „*Übermittlung nur eine begrenzte Zahl von betroffenen Personen betreffen*“[118] darf. Dieser Auffangtatbestand ist gerade kein „*Freifahrtschein*“.[119]

Es ist wichtig zu betonen, dass offenbar die EK selbst die immense Bedeutung der Drittstaatenproblematik verkannt hat.[120] Konkret hat der EDSB[121] vor wenigen Wochen die

---

[108] Die EK hat in ihrem Angemessenheitsbeschluss auch Section 702 des FISA berücksichtigt, allerdings nur in seiner bisherigen Sprachfassung. Insb wurde die Definition von „*Anbietern elektronischer Kommunikationsdienste*“ (engl „*electronic communication service provider*“) maßgeblich erweitert. Daher muss in den TIA der neue Wortlaut berücksichtigt und bestehende TIA dementsprechend aktualisiert werden; vgl hierzu *Kastelitz*, FISA 702: USA Cloud-Überwachung wurde verlängert, abrufbar unter <https://researchinstitute.at/fisa-cloud-ueberwachung-vor-der-verlaengerung/> (24.6.2024); *Golland*, Anforderungen an Transfer Impact Assessments bei Datentransfers in unsichere Drittländer, DSB 2021, 229 (229).

[109] *Knyrim/Gerhalter* in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020) Kap 7 Rz 7.69 ff.

[110] *Leitinger*, DSGVO-konforme Datenübermittlung in die USA, ecolex 2021/382, 589 (589).

[111] *Knyrim/Reisinger*, Internationaler Datentransfer, RDB Keywords Rz 5 (Stand 13.6.2023, rdb.at).

[112] *Jahnel/Pallwein-Prettner*, Datenschutzrecht[3] (2021) 91.

[113] *Knyrim/Gerhalter* in *Knyrim* (Hrsg), DatKomm Art 49 Rz 53 (Stand 1.10.2023, rdb.at).

[114] *Zerdick* in *Ehmann/Selmayr* (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 49 Rz 18.

[115] *Pauly* in *Paal/Pauly* (Hrsg), DS-GVO/BDSG[3] (2021) Art 49 Rz 29.

[116] Vgl Punkt 8 Privacy Policy: OpenAI beruft sich auf berechtigte Interessen von sich, Dritten und (sogar) der Gesellschaft im Allgemeinen, um seine Modelle zu trainieren und zu verbessern; vgl auch OpenAI General FAQ, How ChatGPT and our language models are developed, abrufbar unter <https://help.openai.com/ en/articles/7842364-how-chatgpt-and-our-language-models-are-developed> (12.4.2024): Die zum Training verwendeten Daten sind ua „*nicht dazu gedacht, Einzelpersonen negativ zu beeinflussen*“ und es sei daher angebracht, sich „*bei der Erhebung und Verarbeitung personenbezogener Daten, die in Trainingsinformationen enthalten sind, auf legitime Interessen gem Datenschutzgesetzen wie der DSGVO*“ zu stützen.

[117] *Klug* in *Gola/Heckmann* (Hrsg), DS-GVO/BDSG[3] (2022) Art 49 Rz 13.

[118] *Towfigh/Ulrich* in *Sydow/Marsch* (Hrsg) DS-GVO/BDSG[3] (2022) Art 49 Rz 16, 18.

[119] *Schröder* in *Kühling/Buchner* (Hrsg), DS-GVO/BDSG[4] (2024) Art 49 Rz 43.

[120] *Golland*, Auf ein Word ..., DSB 2024, 85 (85).

[121] EDSB 8.3.2024, EDPS Investigation into use of Microsoft 365 by the European Commission, Case 2021-0518, abrufbar unter <https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf> (12.4.2024); vgl auch EDSB 11.3.2024, European Commission’s use of Microsoft 365 infringes

Verwendung von Microsoft 365 durch die EK als nicht mit der VO (EU) 2018/1725[122] vereinbar beurteilt. Bis zum 9.12.2024 muss die EK nun diverse Datentransfers unterlassen und die Verarbeitungsvorgänge datenschutzkonform ausgestalten.[123]

2.3 Training von KI (am Beispiel von ChatGPT)

2.3.1 Nutzung privater ChatGPT-Accounts

Bei KI-Systemen ist die datenschutzrechtliche Rollenverteilung[124] oft äußerst unterschiedlich.[125] Im vorhin genannten Beispiel ist „*OpenAI Irland*" im Allgemeinen als Verantwortlicher und „*OpenAI USA*" als Auftragsverarbeiter iSd DSGVO zu qualifizieren. Allerdings gilt ein (werbetreibendes) Unternehmen als gemeinsamer Verantwortlicher, wenn es seinen Mitarbeitern die Verwendung privater Accounts für berufliche Zwecke gestattet und konsequenterweise für deren Verstöße gegen die DSGVO einzustehen hat.[126] Eigentlich müssten in solchen Fällen daher Vereinbarungen gem Art 26 DSGVO[127] zwischen dem werbetreibenden Unternehmen und OpenAI abgeschlossen werden;[128] ein Umstand, welcher in der Praxis so gut wie immer vernachlässigt wird.[129]

Unproblematisch ist es, wenn Mitarbeiter ChatGPT um die Beantwortung reiner Wissensfragen ohne Personenbezug bitten (zB könnte der Dienst dazu verwendet werden, bloß

data protection law for EU institutions and bodies, EDPS/2024/05, abrufbar unter <https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf > (12.4.2024).

122 VO (EU) 2018/1725, ABl 2018/L 295, 39.

123 *Korte*, EDSB: Kritik an Einsatz von Microsoft 365 bei der EU-Kommission, ZD-Aktuell 2024, 01629 (beck-online).

124 *Jahnel*, Datenschutzrechtliche Grenzen des Einsatzes von KI-unterstützten Legal Tech Tools, ÖZW 2023, 117 (117).

125 Eine KI selbst kommt – mangels Rechtspersönlichkeit – als Verantwortlicher (noch) nicht in Frage, da dies nur eine „*natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle*" sein kann (Art 4 Z 7 DSGVO).

126 *Schröder* in *Schröder* (Hrsg), Datenschutzrecht für die Praxis[5] (2023) 208.

127 *Abplanalp/Zopf* in *Forgó* (Hrsg), Grundriss Datenschutzrecht (2019) 54.

128 *Conrad*, Künstliche Intelligenz und die DSGVO – Ausgewählte Problemstellungen, KuR 2018, 741 (743).

129 Anderes kann (nur) gelten, wenn das Unternehmen den Mitarbeitern – zB in einer internen „*KI-Policy*" – die arbeitsrechtliche Weisung erteilt hat, private Accounts nicht für berufliche Zwecke zu verwenden und sich der Mitarbeiter diesem Verbot treuwidrig widersetzt. In derartig gelagerten Konstellationen ist es vertretbar, eine alleinige Verantwortlichkeit des Mitarbeiters im Außenverhältnis anzunehmen und diesen gegenüber Dritten für DSGVO-Verstöße haften zu lassen bzw das Unternehmen von einer Haftung zu befreien. Ein Arbeitnehmer wird seinen Arbeitgeber überdies – wegen seiner Treuepflicht und des Haftungsrisikos für das Unternehmen – auf den (geplanten) Einsatz von privaten ChatGPT-Accounts hinweisen müssen.

allgemeine Informationen über Produkte bereitzustellen: „*Erkläre mir mehr über die verschiedenen Funktionen des neuen Smartphones von XY*“; „*Was ist personalisierte Werbung? Welche Vor- und Nachteile hat der KI-Einsatz in der Werbung?*“). Des Weiteren ist es datenschutzkonform, wenn Mitarbeiter ChatGPT einsetzen, um unpersönliche Werbeslogans zu kreieren (zB „*Entdecke das Neue - ohne deine Privatsphäre zu opfern!*").[130] Anders verhält es sich, sobald personenbezogene Daten ins Spiel kommen (zB „*Welche unserer Brillen könnten Frau R besonders gefallen? Berücksichtige dabei insb ihr bisheriges Einkaufsverhalten, Geschlecht, Alter und Aussehen. Erstelle eine personalisierte Werbeanzeige, der sie nicht widerstehen kann und entwirf auch ein passendes Bild, das sie mit der neuen Brille zeigt. Ich lade gleich im Anschluss ihr Foto aus unserer Kundendatenbank hoch. Hier noch eine Zusatzinformation: Wie uns Frau R neulich persönlich mitteilte, leidet sie an Astigmatismus*“).

Verfehlt wäre es, eine bloße Auftragsverarbeiterrolle von OpenAI zu erwägen,[131] weil es sämtlichen Input intern zu Trainingszwecken seiner Dienste weiterverarbeitet.[132] Denn bei der Nutzung privater Accounts für den persönlichen oder beruflichen Gebrauch sehen die AGB[133] lediglich ein Opt-Out vor: „*Wir können Ihre Inhalte weltweit nutzen, um unsere Dienste bereitzustellen, aufrecht zu erhalten, zu entwickeln und zu verbessern, geltende Gesetze einzuhalten, unsere Bedingungen und Richtlinien durchzusetzen und unsere Dienste sicher zu halten. Wenn Sie nicht möchten, dass wir Ihre Inhalte zum Trainieren unserer Modelle verwenden, haben Sie die Möglichkeit, dies zu verhindern, indem Sie Ihre Kontoeinstellungen aktualisieren*.“ Nutzer müssen also die (Weiter-)Verarbeitung der Eingaben und Uploads für Zwecke der laufenden Verbesserung der Dienste von OpenAI eigens deaktivieren.[134]

Dieses Vorgehen ist aus folgenden Gründen DSGVO-widrig. Zum einen konterkariert dieses Verhalten die zuvor erwähnte *Planet49*-Entscheidung des EuGH,[135] die besagt, dass vorangekreuzte Auswahlfelder verboten sind. Zum anderen verstößt es gegen den Grundsatz „*Privacy*

[130] *Bisset/Schreiber*, ChatGPT und Datenschutz, AnwBl 2023/308, 649 (649).
[131] *Stadler/Bauer/Chochola* in *Bichler* (Hrsg), Praxishandbuch Marketingrecht (2024) 258 ff.
[132] *Wilmer*, Rechtsfragen bei ChatGPT & Co., KuR 2023, 233 (233).
[133] Vgl OpenAI Nutzungsbedingungen für Europa.
[134] Vgl OpenAI Policy FAQ, How your data is used to improve model performance, abrufbar unter <https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance> (12.4.2024): Ein Opt-Out bewirkt (nur), dass neue Konversationen nicht zum Trainieren verwendet werden; vgl OpenAI Data Controls FAQ, abrufbar unter <https://help.openai.com/en/articles/7730893-data-controls-faq> (12.4.2024): Hier wird beschrieben, wie ein Nutzer sein Opt-Out wahrnehmen kann.
[135] EuGH 1.10.2019, C-673/17 (*Planet49*).

by Default" (Art 25 Abs 2 DSGVO), wonach die Einstellungen eines Systems bzw einer Anwendung standardmäßig auf die datenschutzfreundlichste Stufe eingestellt sein müssen.[136]

Bei der Verarbeitung ist es außerdem essenziell, sicherzustellen, dass nur die für den hinreichend bestimmten Verarbeitungszweck unbedingt erforderlichen Daten verarbeitet werden („*Zweckbindung*": Art 5 Abs 1 lit b DSGVO).[137] Bloß allgemeine Hinweise wie zB „*Marketingzwecke*" genügen nicht. Ebenfalls unzureichend ist es, Daten aus verschiedenen Quellen zu sammeln und für Big Data-Analysen zu verwenden, ohne spezifische Zwecke anzugeben. Dementsprechend können auch vage Angaben wie die „*allgemeine Wissensmehrung*" oder die „*zufällige Identifikation von Korrelationen*" nicht als ausreichend bestimmt betrachtet werden.[138] Ferner missbilligte schon die ehemalige Art-29-Datenschutzgruppe[139] Formulierungen wie „*Verbesserung der Nutzererfahrung*", „*IT-Sicherheitsangelegenheiten*" oder „*zukünftige Forschung*". OpenAI wird dem Bestimmtheitsgebot nicht gerecht, weil die angegebenen Zwecke zu abstrakt formuliert sind.[140]

Abseits dessen muss eine Datenverarbeitung immer auf das notwendige Minimum beschränkt sein, sowohl in Bezug auf die Menge der erhobenen Daten als auch den Umfang der Verarbeitung, die Speicherfristen und den Zugang zu den Daten („*Datenminimierung*": Art 5 Abs 1 lit c DSGVO).[141] Dies ist durch geeignete TOM für alle Phasen des KI-Einsatzes umzusetzen.[142] Im Grunde genommen sollte das Bewusstsein der Betroffenen durch die Implementierung eines Opt-In geschärft werden, das wesentlich darauf abzielt, die Unerfahrenheit und Unwissenheit der Nutzer beim Umgang mit Big Data-Anwendungen auszugleichen.[143]

---

136 *Bergauer* in *Jahnel* (Hrsg), DSGVO Art 25 Rz 20 ff (Stand 1.12.2020, rdb.at).

137 *Alon*, KI in der Gesundheitstechnologie: Die Datenschutz-Challenge, GRC aktuell 2023, 93 (94 ff).

138 *Roßnagel* in *Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 5 Rz 88.

139 Art-29-Datenschutzgruppe 2.4.2013, WP 203, Stellungnahme 03/2013 zur Zweckbindung, 16, abrufbar unter <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (16.4.2024).

140 Vgl Punkt 8 Privacy Policy: OpenAI stützt sich auf berechtigte Interessen „*zur Verbesserung und Entwicklung [der] Dienste und neuer Funktionen sowie zur Durchführung von Forschung.*" Ergänzend werden in Punkt 3 Privacy Policy weitere Zwecke angegeben, wie zB die Analyse der Effektivität der Dienste, das Hinzufügen neuer Funktionen oder „*andere ähnliche Zwecke*". Offen bleibt mE, welche Bedeutung va letzteren zukommt.

141 *Kinast/Stanonik* (Hrsg), Praxishandbuch Datenschutz für KMU (2019) 68, 71 f.

142 *Anderl/Ciarnau*, Datenschutzrechtliche Herausforderungen bei Generativer KI, ecolex 2023/667, 1078 (1078).

143 *Abplanalp/Zopf* in *Forgó* (Hrsg), Grundriss Datenschutzrecht (2019) 80 f.

Abgesehen davon ist zu berücksichtigen, dass eine Weiterverarbeitung für Trainingszwecke eine Rechtsgrundlage iSd DSGVO benötigt.[144] Ob allerdings eine neue Rechtsgrundlage erforderlich ist oder ob die Weiterverarbeitung noch durch die ursprüngliche gedeckt ist, ist in der Literatur äußerst umstritten.[145] Dabei überzeugt die Meinung von *Bierbauer*,[146] welcher annimmt, dass eine neue Rechtsgrundlage aus Rechtssicherheitsgründen erforderlich ist. Art 6 Abs 4 DSGVO (iVm ErwGr 50 DSGVO) bildet in dieser Hinsicht keine ausreichende Basis.[147] Insb wird der „*Kompatibilitätstest*"[148] – also die Prüfung, ob die Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Zweck vereinbar ist – regelmäßig ergeben, dass die „*vernünftigen Erwartungen*"[149] der Betroffenen nicht ausreichend berücksichtigt wurden. Anlässlich der Verarbeitung personenbezogener Daten in Situationen, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen musste, hat eine Interessenabwägung zugunsten des Betroffenen auszufallen (vgl ErwGr 47 DSGVO). Konnte ein Betroffener bei der Datenerhebung mithin davon ausgehen, dass seine Daten nicht für einen nachgelagerten Zweck verarbeitet werden, ist dieser Zweck nicht mit dem Erhebungszweck vereinbar.[150] Das erscheint insofern konsequent, als es mit zunehmender Autonomie der KI und der Entfernung ihrer Verarbeitungsprozesse von der ursprünglichen Zweckfestlegung wahrscheinlicher wird, dass die neuen Zwecke nicht mehr als unmittelbar folgende („*logische*") Schritte erscheinen. Als eingriffsintensive Datenverarbeitungen bedürfen diese einer gesonderten Legitimation.[151] Geht es vordergründig um die ausschließliche Nutzung des kommerziellen Werts der Daten (zB zur Refinanzierung „*kostenloser*" Angebote)[152] ist eine

[144] Zur Vertragserfüllung wird das Training der KI grds nicht erforderlich – iSv objektiv notwendig – sein, außer die Verbesserung wurde eigens als Vertragsbestandteil vereinbart. Eine Einwilligung wird oftmals gar nicht vorliegen (insb wenn personenbezogene Daten Dritter durch ChatGPT verarbeitet werden, die davon keine Kenntnis haben). Außerdem kann sie zu jeder Zeit widerrufen werden (Art 7 Abs 3 DSGVO), woraufhin darauf basierende Trainingsdatensätze gelöscht werden müssten (Art 17 Abs 1 lit b DSGVO), was sich bei KI-Modellen idR als nicht umsetzbar erweisen wird; vgl auch *Helminger*, Datenschutzrechtliche Herausforderungen bei der Verwendung von Trainingsdaten, EALR 2022, 46 (46); *Gausling*, Künstliche Intelligenz und DSGVO, DSRITB 2018, 519 (519, 531).

[145] Dafür zB *Bergauer*, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DSGVO, jusIT 2018/83, 231 (232 ff); aA zB *Raji*, Privilegiertes Training von KI-Systemen, DSB 2022, 193 (193) und *Krügel/Pfeiffenbring* in *Ebers/Heinze/Krügel/Steinrötter* (Hrsg), Künstliche Intelligenz und Robotik (2020) § 11 Rz 25.

[146] *Bierbauer* in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2021 (2022) 175.

[147] Vgl Kapitel 3.7.3 (KI-Reallabore & Datenschutz): Art 59 KI-VO.

[148] *Duisberg* in *Borges/Keil* (Hrsg), Rechtshandbuch Big Data (2024) § 6 Rz 61.

[149] *Feiler/Forgó*, EU-DSGVO und DSG[2] (2022) Art 6 Rz 30.

[150] *Taeger* in *Taeger/Gabel* (Hrsg), DSGVO/BDSG/TTDSG[4] (2022) Art 6 Rz 177.

[151] *Buchner/Petri* in *Kühling/Buchner* (Hrsg), DS-GVO/BDSG[4] (2024) Art 6 Rz 187.

[152] *Schmidt-Kessel/Grimm*, Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten, ZfPW 2017, 84 (86 ff).

Vereinbarkeit mit dem ursprünglichen Zweck der Datenverarbeitung auf jeden Fall abzulehnen.[153] Überdies ist im Rahmen von Big Data- bzw Data Mining-Analysen eine Weiterverarbeitung zu „*Statistikzwecken*" (vgl Art 89 DSGVO iVm ErwGr 162 Satz 5 DSGVO) nicht kompatibel mit den ursprünglichen Zwecken, weil „*die statistischen Zwecke durch wirtschaftliche Zwecksetzungen überlagert werden*."[154] Weiters muss der Verantwortliche bei der Vereinbarkeitsprüfung von Big Data-Analysen besonderes Augenmerk darauf legen, dass durch die Kombination von Daten aus verschiedenen Kontexten neue Zusammenhänge sichtbar werden können.[155]

Eine Zweckänderung gestaltet sich idR weniger problematisch, solange die Daten ausreichend geschützt sind. Datensicherheit, technische Schutzmaßnahmen vor Cyberangriffen und organisatorische Beschränkungen von Zugriffsberechtigungen haben diesbezüglich einen herausragenden Stellenwert.[156] Schwieriger wird es jedoch, wenn Big Data-Analysen darauf abzielen, neue Erkenntnisse über betroffene Personen zu gewinnen oder wenn die erlangten Ergebnisse direkte Folgen für Betroffene haben, wie bspw Entscheidungen zu ihrem Nachteil.[157] Explorative Big Data-Analysen, bei denen die zu stellenden Fragen erst aus dem Analyseergebnis selbst hervorgehen, sind demgemäß mit dem Grundsatz der Zweckbindung unvereinbar. Daher sollten sie ausschließlich mit nicht-personenbezogenen Daten oder anonymisierten Daten durchgeführt werden.[158] Die Anonymisierung kann uU eine zulässige Weiterverarbeitungsform darstellen, sofern das dafür angewandte Verfahren geeignet ist, verlässlich anonymisierte Informationen zu generieren.[159]

Der Vollständigkeit halber sollen deshalb noch weitere – aus meiner Sicht heikle – Punkte der Datenschutzerklärung veranschaulicht werden. OpenAI betont zunächst, dass es

---

[153] *Roßnagel* in *Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 6 Rz 38.

[154] *Skistims* in *Kaulartz/Braegelmann* (Hrsg), Rechtshandbuch Artificial Intelligence und Maschine Learning (2020) Kap 8.2 Rz 61.

[155] *Raabe/Wagner*, Verantwortlicher Einsatz von Big Data, DuD 2016, 434 (438).

[156] *Grünbichler/Salimbeni*, Künstliche Intelligenz in Unternehmen: Eine Kategorisierung der Implementierungshürden, GRC aktuell 2023, 127 (127).

[157] Art-29-Datenschutzgruppe 2.4.2013, WP 203, Stellungnahme 03/2013 zur Zweckbindung, 45.

[158] *Valkanova* in *Kaulartz/Braegelmann* (Hrsg), Rechtshandbuch Artificial Intelligence und Maschine Learning (2020) Kap 8.1 Rz 10.

[159] Art-29-Datenschutzgruppe 10.4.2014, WP 216, Stellungnahme 5/2014 zu Anonymisierungstechniken, 8, abrufbar unter <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (18.4.2024).

personenbezogene Daten anonymisiert bzw aggregiert,[160] sodass Nutzer nicht mehr identifiziert werden können. Das Unternehmen *„wird [auch] nicht versuchen, die Daten wieder zu re-identifizieren."* Doch allein die Tatsache, dass dazu noch die Möglichkeit besteht, läuft per se dem Sinn und Zweck einer Anonymisierung zuwider. Die Wiederherstellung des Personenbezugs sollte eigentlich (va bei Dritten) nicht mehr möglich sein. Eine Re-Identifizierung wird durch OpenAI auch dann durchgeführt, wenn dies „*gesetzlich gefordert*" ist. Infolgedessen können diese – bloß scheinbar anonymisierten – Daten erst recht den US-Behörden gem den amerikanischen Überwachungsgesetzen zugänglich gemacht werden. Das von OpenAI abgegebene Versprechen,[161] dass die Entwicklung seiner Dienste mit Datenschutzgesetzen in Einklang steht, ist somit als ein reines Lippenbekenntnis zu werten.

Daneben ist ein Konflikt mit dem Grundsatz der „*Speicherbegrenzung*" (Art 5 Abs 1 lit e DSGVO)[162] erkennbar, denn OpenAI gibt in Punkt 5 („*Speicherung*") seiner Privacy Policy an: „*Wir werden Ihre personenbezogenen Daten nur so lange speichern, wie wir sie benötigen, um Ihnen unseren Dienst zur Verfügung zu stellen oder für andere legitime Geschäftszwecke*." Nachfolgend werden Streitbeilegung, Sicherheitsgründe und die Erfüllung von Rechtspflichten als Beispiele für „*legitime Geschäftszwecke*" genannt; zu denken sei etwa an gesetzliche Aufbewahrungspflichten aus dem Unternehmens- oder Steuerrecht. Jedoch ist dieser Katalog nicht abschließend. Darüber hinaus wird die Dauer der Datenspeicherung von weiteren Faktoren – ua den jeweiligen Einstellungen – abhängig gemacht: Bleibt ein privater Nutzer untätig, sodass Daten standardmäßig zum Training der KI verwendet werden, kommt es zu keiner Löschung. Das steht offensichtlich im Widerspruch zu den Verarbeitungsgrundsätzen. Daten, die ursprünglich für einen spezifischen Zweck erhoben wurden, werden nunmehr für die KI-Entwicklung „*auf Vorrat*" gespeichert. Sobald die Verarbeitung für den anfänglichen Zweck nicht mehr erforderlich ist, sollte die Speicherung aber nicht unnötig verlängert werden.[163] Wird der Chatverlauf dagegen deaktiviert, löscht OpenAI neue Konversationen (erst) nach 30

[160] Vgl Punkt 3 Privacy Policy.

[161] Vgl OpenAI General FAQ, How ChatGPT and our language models are developed; OpenAI GPTs Data Privacy FAQs, abrufbar unter <https://help.openai.com/en/articles/8554402-gpts-data-privacy-faqs> (13.4.2024).

[162] Vgl ErwGr 39 DSGVO: Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert, dass die Speicherfrist auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Wird der Zweck der Verarbeitung erreicht, sind die Daten grds sofort zu löschen; vgl *Paal* in *Kaulartz/Braegelmann* (Hrsg), Rechtshandbuch Artificial Intelligence und Maschine Learning (2020) Kap 8.7 Rz 16.

[163] *Bierbauer* in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2021 (2022) 175.

Tagen. Von der propagierten „*Dauerhaftigkeit*" kann in diesem Zusammenhang nicht gesprochen werden, weil OpenAI weiterhin Zugriff hat, um *„bei Bedarf Missbrauch zu überwachen und zu untersuchen*." Eine alternative Möglichkeit für OpenAI, seiner Löschpflicht nachzukommen, wäre die beschriebene Anonymisierung der Daten.[164] Allerdings sind Nutzer dabei der zuvor dargestellten Gefahr ausgesetzt, dass US-Behörden die Offenlegung der vermeintlich anonymen Daten aufgrund gesetzlicher Anordnungen verlangen könnten.

Abschließend stellt das Problem der „*Halluzination*" von Output durch KI-Systeme ein ernsthaftes Anliegen dar.[165] Gemäß der DSGVO müssen personenbezogene Daten sachlich richtig und auf dem neuesten Stand sein. Daten, die unrichtig sind, müssen stattdessen korrigiert oder gelöscht werden (Art 5 Abs 1 lit d DSGVO: „*Datenrichtigkeit*"). Erstaunlicherweise hat OpenAI selbst zugegeben, dass es schwierig – wenn nicht sogar unmöglich – ist, unwahre Informationen in KI-Systemen zu korrigieren. Weiters fehlt es an Transparenz darüber, welche Informationen über Individuen gespeichert werden und woher diese Informationen stammen. Es ist deswegen nicht verwunderlich, dass Noyb eine Beschwerde bei der österreichischen DSB eingebracht hat.[166] Dem Unternehmen ist es bisher nicht gelungen, eine DSGVO-Konformität in dieser Hinsicht herzustellen.[167]

2.3.2 Nutzung betrieblicher ChatGPT-Accounts

Im Gegensatz zur Verwendung privater Accounts gestaltet sich die datenschutzrechtliche Ausgangslage für Unternehmen, welche ChatGPT über APIs integrieren[168] oder für ihre Arbeitnehmer Business-Accounts anlegen, wesentlich einfacher.[169] Das Unternehmen fungiert als

[164] DSB 5.12.2018, D123.270/0009-DSB/2018: Anonymisierung statt Löschung ist uU zulässig.

[165] *Aschauer*, (Juristische) Anwendungsmöglichkeiten von Large Language Models, RZ 2024, 15 (15).

[166] Noyb 29.4.2024, ChatGPT provides false information about people, and OpenAI can't correct it, abrufbar unter <https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it> (29.4.2024).

[167] Reuters 24.5.2024, EU data protection board says ChatGPT still not meeting data accuracy standards, abrufbar unter <https://www.reuters.com/technology/eu-data-protection-board-says-chatgpt-still-not-meeting-data-accuracy-standards-2024-05-24/> (21.6.2024).

[168] So wäre es zB möglich, hauseigene Chatbots zu entwickeln, die wiederkehrende Fragen automatisch beantworten. Ebenso könnten verschiedene Legal Tech-Tools so gestaltet werden, dass sie für präzise juristische Recherchen verwendet werden können; vgl *Lobinger*, (Chat-)GPT in der juristischen Leistungserbringung – Möglichkeiten und Grenzen, LTZ 2023, 187 (187); *Eisenberger* in *Hofmann/Hölscheidt/Mörth/Pirker/Pöschl/Wiederin* (Hrsg), FS Merli (2023) 807.

[169] *Bisset*, KI und Datenschutz (Stand 17.1.2024, Lexis Briefings in lexis360.at).

Verantwortlicher, während OpenAI als reiner Auftragsverarbeiter agiert.[170] Von einer gemeinsamen Verantwortlichkeit ist nicht auszugehen, weil OpenAI Nutzerinhalte im B2B-Verhältnis nicht zu Trainingszwecken seiner Dienste weiterverarbeitet.[171] Nichtsdestotrotz haben Unternehmen die Gelegenheit, sich für ein Opt-In zu entscheiden und insofern OpenAI freiwillig ihre Daten zur Verfügung zu stellen. Aus datenschutzrechtlicher Perspektive ist davon abzuraten.

Letztendlich ist ein AVV (Art 28 Abs 3 DSGVO)[172] abzuschließen und das konkrete Verhältnis überdies im jeweiligen VVT (Art 30 DSGVO)[173] festzuhalten. Wiederum wird dies in der Praxis wahrscheinlich nicht ausreichend berücksichtigt werden. Hinzukommend muss Unternehmen bewusst sein, dass personenbezogene Daten in die USA übertragen werden, sodass es entscheidend ist, die Vorgaben der Art 44 ff DSGVO einzuhalten (zur Drittstaatenproblematik siehe bereits oben). Zu guter Letzt ist darauf hinzuweisen, dass möglicherweise eine Pflicht zur Durchführung einer DSFA (Art 35 DSGVO) besteht.[174] Da KI-Systeme im Allgemeinen als neue Technologien angesehen werden, bei denen (noch) nicht vollständig geklärt ist, welche potenziell risikoreichen Auswirkungen sie auf betroffene Personen und die Gesellschaft als Ganzes haben könnten, ist eine DSFA im Grunde genommen unvermeidlich (vgl § 2 Abs 2 Z 4 DSFA-V).[175]

2.3.3 Zwischenfazit

Zur Zeit gibt es aus all diesen Gründen kaum eine sichere Möglichkeit für Unternehmen, ChatGPT und andere OpenAI-Dienste zu nutzen und zugleich DSGVO-konform zu bleiben.[176] Der Einsatz von KI stellt alle Grundsätze der Datenverarbeitung gem Art 5 und Art 25 DSGVO vor (noch) unlösbare Herausforderungen, wodurch die vollständige Einhaltung dieser Vorschriften nicht garantiert werden kann. Obwohl den Verantwortlichen (das Unternehmen) eine Rechenschaftspflicht trifft (Art 5 Abs 2 DSGVO), wird es ihm konsequenterweise schwerfallen, sowohl

[170] *Sedef/Steiner*, Datenschutz - Auftragsverarbeiter (Stand 11.3.2024, Lexis Briefings in lexis360.at).
[171] Vgl OpenAI Enterprise Privacy (Stand 10.1.2024), abrufbar unter <https://openai.com/enterprise-privacy> (18.4.2024); vgl OpenAI Business Terms (Stand 14.11.2023), abrufbar unter <https://openai.com/policies/business-terms> (18.4.2024).
[172] *Bogendorfer* in *Knyrim* (Hrsg), DatKomm Art 28 Rz 65 (Stand 1.12.2022, rdb.at).
[173] *Bogendorfer* in *Knyrim* (Hrsg), DatKomm Art 30 Rz 15 ff (Stand 1.12.2022, rdb.at).
[174] *Schneeberger*, Intelligente Medizinprodukte: Rechtsfragen am Schnittpunkt von DSGVO, MPVO und AI Act, Dako 2024/3, 4 (4).
[175] DSFA-V, BGBl II Nr 278/2018: Bestimmte Verarbeitungsvorgänge erfordern eine DSFA (sog „*Blacklist*“).
[176] *Weiss*, Artikelserie ChatGPT im Kanzleialltag nutzen, AnwBl 2024/119, 234 (234).

Transparenz zu gewährleisten und seinen Informationspflichten (Art 13 f DSGVO) nachzukommen, als auch die Ausübung der Betroffenenrechte (Art 15 ff DSGVO) durch geeignete Maßnahmen zu unterstützen (vgl Art 12 Abs 2 DSGVO). Sollte der Verantwortliche jedoch nicht sicherstellen können, dass die Betroffenenrechte eingehalten werden können, darf er das entsprechende KI-System von vornherein nicht einsetzen.

Insb da die meisten KI-Systeme als sog „*Blackbox*" gelten,[177] werden Unternehmen keine (detaillierte) Auskunft über die Datenverarbeitungen und va nicht über den zugrundliegenden (komplexen) Algorithmus, die Tragweite und Auswirkungen des Systems für betroffene Personen geben können. Eine rechtskonforme Einwilligung einzuholen, scheitert daher im Allgemeinen am Erfordernis der „*Informiertheit*" des Betroffenen. Selbst wenn man berechtigterweise davon ausgeht, dass der Algorithmus an sich nicht offengelegt werden muss, sollte zumindest eine „*verständliche*" Darlegung der Funktionsweise und der primär angedachten (bestimmungsgemäßen) Einsatzgebiete in „*klarer und einfacher Sprache*" erfolgen (vgl Art 12 Abs 1 DSGVO). Die konkrete Umsetzung dieser Vorgaben in der Praxis ist jedoch noch nicht geklärt. Offen ist, wie durchschnittlichen, technisch nicht versierten Betroffenen – insb Kindern – der Einsatz von KI leicht verständlich erklärt werden kann. Dazu muss ein KI-Betreiber selbst die Funktionsweise und die Entscheidungen der KI ausreichend verstehen.[178] Besonders fragwürdig ist zudem die technische Realisierung der Rechte auf Berichtigung und Löschung („Vergessenwerden").[179] Schon aus diesen Gründen ist es ratsam, (derzeit) vom Einsatz von ChatGPT und ähnlichen KI-Systemen Abstand zu nehmen.

In Anbetracht des problematischen Drittstaatenbezugs sollten Unternehmen des Weiteren Priorität darauf legen, zu Anbietern in der EU zu wechseln, die ein ausschließliches EU-Hosting garantieren.[180] Aufgrund des Cloud Act ist auch ein Ausweichen auf Cloud-Lösungen nicht anzuraten.

---

[177] *Neufeld*, ChatGPT – das Ende der Unschuld, BB 2023 H 7, I (I).

[178] Die durch die KI-VO eingeführten Transparenz- und Informationspflichten für KI-Anbieter könnten KI-Betreibern dabei helfen, detaillierte Einblicke in die implementierten Systeme zu erhalten (vgl ua Art 13, 20, 49 und Art 79 Abs 13-14 KI-VO für Hochrisiko-KI, Art 50 Abs 1-2 KI-VO für KI-Systeme mit geringem Risiko sowie Art 53 und Art 55 KI-VO für GPAI). Es ist auch sinnvoll, einen gründlichen Blick in die AGB und die Privacy Policy des KI-Anbieters zu werfen.

[179] *Aichinger/Leitner* in *Mayrhofer/Nessler/Bieber/Fister/Homar/Tumpel* (Hrsg), ChatGPT, Gemini & Co (2024) 164.

[180] *Hersemeyer/Ludolph*, Datenschutzrechtliche Herausforderungen beim Einsatz Künstlicher Intelligenz im Unternehmenskontext, InTeR 2024, 55 (55).

Unternehmen sollten darüber hinaus immer prüfen, ob und inwieweit Daten zu Trainingszwecken durch den KI-Anbieter weiterverarbeitet werden. Es könnte insofern eine gemeinsame Verantwortlichkeit mit dem KI-Anbieter bestehen. Es bräuchte dann weitgehende Überlegungen zur DSGVO-konformen Ausgestaltung von Datenschutzerklärungen und -verträgen. Die Entwicklung von GPAI erfordert zwangsläufig die Verwendung riesiger Datenmengen,[181] sodass auch die Aufnahme personenbezogener oder urheberrechtlich geschützter Daten sowie von Texten mit fragwürdigem, falschem oder diskriminierendem Inhalt (zB Desinformation, Propaganda oder Hassbotschaften) in den Trainingsdatensatz nicht ausgeschlossen werden kann.[182] Ein denkbarer Ansatz wäre es zB, wenn um die Einwilligung der Betroffenen in die Weiterverarbeitung ihrer personenbezogenen Daten ersucht wird und diese erhobenen Daten anschließend zu Trainingszwecken anonymisiert werden, sodass der Personenbezug auch durch den Einsatz von KI nicht wiederherstellbar ist.

Sich auf berechtigte Interessen zu stützen, ist dagegen nicht empfehlenswert. Meta erlebte dies kürzlich, als das Unternehmen bei der Entwicklung und dem Training der sog „*Meta AI*" auf sein angeblich berechtigtes Interesse verwies.[183] Das Vorgehen von Meta verstieß derart gegen die DSGVO, dass es – vermutlich aufgrund des starken Widerstands der Zivilgesellschaft und mehrerer Beschwerden bei den DSB – schließlich einsah, dass die Verwendung personenbezogener Daten von EU-Bürgern für das KI-Training auf diesem Weg nicht zulässig war.[184] Dabei hätte Meta lediglich die Einwilligung der Nutzerinnen (Opt-In) einholen müssen, wie es auch die norwegische DSB in einer ersten Stellungnahme andeutete.[185] Diesen Schritt wollte Meta jedoch unbedingt vermeiden und entschied sich stattdessen für einen rechtswidrigen Ansatz.

---

[181] *Gausling* in *Ballestrem/Bär/Gausling/Hack/von Oelffen* (Hrsg), Künstliche Intelligenz (2020) 13.

[182] BSI, Generative AI Models - Opportunities and Risks for Industry and Authorities[v1.1], 9, abrufbar unter <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Generative_AI_Models.pdf?__blob=publicationFile&v=4> (19.4.2024).

[183] *Noyb* 6.6.2024, noyb fordert 11 Behörden auf, Metas Missbrauch persönlicher Daten für KI zu stoppen, abrufbar unter <https://noyb.eu/de/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai> (21.6.2024).

[184] *Noyb* 14.6.2024, (Vorläufiger) noyb-Sieg: Meta stoppt KI-Pläne in der EU, abrufbar unter <https://noyb.eu/de/preliminary-noyb-win-meta-stops-ai-plans-eu> (21.6.2024).

[185] Norwegische DSB 4.6.2024, Meta vil benytte brukernes bilder og innlegg til å utvikle KI, abrufbar unter <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/meta-vil-bruke-brukernes-bilder-og-innlegg-til-a-utvikle-ki/> (21.6.2024): Die Rechtmäßigkeit der Vorgehensweise von Meta ist zweifelhaft. Nach Ansicht der DSB wäre es am natürlichsten gewesen, die Nutzer um ihre Einwilligung zu bitten.

Entscheidet sich ein Unternehmen trotz der aufgezeigte Risiken für den Einsatz von ChatGPT, sollte zumindest die Nutzung privater Accounts für Mitarbeiter für berufliche Zwecke untersagt werden. Dies ist besonders wichtig aufgrund der möglichen urheber-, haftungs- und datenschutzrechtlichen Konsequenzen, wie etwa Geldbußen in Millionenhöhe für das Unternehmen. Ein solcher Haftungsausschluss für das treuwidrige Verhalten von Mitarbeitern sollte außerdem in einer KI-Policy transparent nach außen kommuniziert werden, bspw durch Bereitstellung eines abrufbaren Dokuments auf der Homepage und Verlinkung in der Datenschutzerklärung.

Bereits jetzt wird darauf hingewiesen, dass es zur Behebung dieser Rechtsunsicherheiten möglicherweise erforderlich sein könnte, einen „*KI-Beauftragten*“[186] neben einem DSBA zu bestellen,[187] um Verantwortlichkeiten innerhalb des Unternehmens klar zuzuweisen.[188] Eine sinnvolle Ergänzung können interne Leitlinien und Schulungsmaßnahmen bzgl des Umgangs mit KI-Systemen bilden. Unterstützung und Beratung bietet seit Kurzem auch die „*KI-Servicestelle*“, welche in Österreich bei der RTR-GmbH eingerichtet wurde.[189]

[186] Aus der KI-VO selbst geht keine unmittelbare Pflicht zur Bestellung eines KI-Beauftragten hervor. Anbieter und Betreiber von KI-Systemen müssen aber Maßnahmen ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen (Art 4 KI-VO). „*KI-Kompetenz*“ sind die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen der KI-VO ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden (Art 3 Z 56 KI-VO; vgl auch ErwGr 2, 20, 91, 165 KI-VO).

[187] *Riess*, ChatGPT und künstliche Intelligenz, AR aktuell 2023, 129 (129).

[188] DSK 6.5.2024, Orientierungshilfe Künstliche Intelligenz und Datenschutz, Rz 32 ff, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf> (8.5.2024).

[189] RTR, Servicestelle für Künstliche Intelligenz, abrufbar unter <https://www.rtr.at/rtr/service/ki-servicestelle/ki-servicestelle.de.html> (13.4.2024).

2.4 Pay-or-Okay

2.4.1 Hintergrund

In der aktuellen datenschutzrechtlichen Debatte hoch im Kurs stehen außerdem die sog „*PUR-Modelle*" bzw „*Pay-or-Okay*"-Konzepte.[190] Obgleich die DSB[191] deren Zulässigkeit anfangs großzügig beurteilte,[192] wird inzwischen eine abgeschwächte Auffassung vertreten.[193] Zwar fehlen bis dato wegweisende Urteile der EU-Gerichte,[194] doch wird – mE zu Recht – befürchtet, dass eine Unterwanderung des Erfordernisses der Einwilligungserteilung in freiwilliger und informierter Weise droht.[195] Auch das „*Koppelungsverbot*" (Art 7 Abs 4 DSGVO)[196] spielt – ähnlich wie bei Newslettern[197] – eine nicht unwesentliche Rolle.[198] Das Grundrecht auf Privatsphäre und Datenschutz[199] darf jedoch nicht von den finanziellen Verhältnissen der Betroffenen abhängig gemacht werden.[200]

Auf die Spitze trieb dieses Modell schließlich Meta, welches die Erteilung der Einwilligung für die Datenverarbeitung schlicht in seine AGB verlagerte.[201] Die Nutzer mussten diese

[190] Bei diesen wird dem Nutzer die Wahl überlassen, entweder eine Geldsumme für die Inanspruchnahme der angebotenen Online-Inhalte zu zahlen („*pay*") oder eine Einwilligung in Tracking und Analyse, va zur Verarbeitung der Daten für personalisierte Werbung, zu erteilen („*okay*"). Diese Unentgeltlichkeit ist nur eine scheinbare, da man diesfalls mit seinen Daten bezahlt; vgl *Nikol/Rost*, "Pay or okay" - okay or not okay? DSB 2023, 167 (167).

[191] DSB 30.11.2018, D122.931/0003-DSB/2018.

[192] *Schwamberger*, Zulässigkeit von "Pay or Okay", jusIT 2019/31, 88 (89).

[193] DSB 29.3.2023, D124.4574 (2023-0.174.027): Keine „*unverhältnismäßig hohen Preise*".

[194] Vgl *Maran*, Datenschutzkonformes Tracking zu Werbe- und Marketingzwecken, CB 2023, 345 (345): Ausführlich zur Situation in Deutschland.

[195] DSB 16.4.2019, D213.679/0003-DSB/2018: Gerade dann, wenn die Nichterteilung zu einem Nachteil für den Betroffenen führen könnte.

[196] *Kastelitz* in *Knyrim* (Hrsg), DatKomm Art 7 Rz 33 ff (Stand 7.5.2020, rdb.at).

[197] OGH 24.10.2019, 6 Ob 56/19g; *Seeauer* in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2018 (2018) 46 f.

[198] *Wagner* in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2023 (2024) 368; vgl DSB 20.8.2019, D122.974/0001-DSB/2019 und EDSA 4.5.2020, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679$^{v1.1}$, Rz 26 f, 38 ff, 86.

[199] *Eisenberger* in *Österreichischer Juristentag* (Hrsg), Verhandlungen des Einundzwanzigsten Österreichischen Juristentages Wien 2022 I/2 (2024) 146.

[200] *Noyb* 13.8.2021, News Sites: Readers need to "buy back" their own data at an exorbitant price?! abrufbar unter <https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price> (6.4.2024); *Noyb* 11.4.2023, "Pay or Okay" - the beginning of the end? abrufbar unter <https://noyb.eu/en/pay-or-okay-beginning-end> (6.4.2024).

[201] Das Geschäftsmodell von Meta beruht hauptsächlich darauf, sich durch das Ausspielen personalisierter Werbung und kommerzieller Inhalte zu finanzieren.

Nutzungsbedingungen naturgemäß akzeptieren, um die sozialen Netzwerke Facebook und Instagram verwenden zu können. Mit der Akzeptanz der AGB erteilten die Betroffenen folglich auch ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten für Zwecke der maßgeschneiderten Online-Werbung.[202] Zusätzlich wurden Nutzerdaten auf Websites und in Apps von Drittanbietern gesammelt, insb über sog „*Social Plugins*"[203] bzw den bekannten „*Like-Button*".[204]

Diese Aktivitäten wurden von Meta anschließend miteinander verknüpft, um detaillierte Nutzerprofile zu erstellen.[205] Dies erfolgte selbst dann, wenn die Nutzer diesem intensiven Webtracking durch Browser- oder Geräteeinstellungen widersprochen hatten.[206] Das dt BKartA[207] erblickte in diesem Verhalten – neben einem Konditionenmissbrauch[208] – va auch einen Verstoß gegen die DSGVO.[209] Im weiteren Verfahrensverlauf[210] legte das OLG Düsseldorf dem EuGH maßgebliche Fragen zur Vorabentscheidung vor.[211]

Dem daraufhin ergangenen Grundsatzurteil des EuGH[212] zufolge können durch Webtracking erhobene und zusammengeführte Daten für Zwecke der Personalisierung von Inhalten und Werbung grds nicht auf die Rechtsgrundlage des Art 6 Abs 1 lit b DSGVO (Vertragserfüllung) gestützt werden,[213] weil diese idR nicht objektiv unerlässlich ist,[214] um die Vertragsleistung zu verwirklichen.[215] Das berechtigte Interesse (Art 6 Abs 1 lit f DSGVO) scheidet aus, weil die zwingend durchzuführende Interessenabwägung zugunsten der Nutzer auszufallen hat,

---

202 *Kornbeck*, Datenschutzrechtsverstöße als kartellrechtlicher Konditionenmissbrauch, ÖZK 2022, 245 (245).

203 *Frank-Woda/Steiner*, Datenschutz in der Unternehmenspraxis (2022) 185 ff.

204 EuGH 29.7.2019, C-40/17 (*Fashion ID*) Rz 75 ff, 88, 107; *Horak/Spring*, Der Facebook-"Like-Button" benötigt die Zustimmung, ÖBl 2019/76, 291 (291); *Mayer*, Webshop-Recht[2] (2019) 162 f.

205 *Holzweber/Scharf*, Datenmissbrauch im Kartellrecht? Der Fall Facebook, ecolex 2018, 258 (258).

206 *Golland/Kelbch*, Kartellrecht vs. Datenschutzrecht: Rechtsgrundlagen für die Datenverarbeitung in sozialen Netzwerken, DSB 2023, 247 (247).

207 BKartA 6.2.2019, B6-22/16.

208 *Hoffer* in *Binder Grösswang* (Hrsg), Digital Law[2] (2020) 252 f.

209 *Legner*, Entscheidungen zum europäischen Kartellrecht im Jahr 2023, GPR 2024, 37 (Rz 13).

210 *Jaeger*, Europarecht: Das Neueste auf einen Blick, wbl 2023, 555 (556 ff).

211 OLG Düsseldorf 24.3.2021, VI-Kart 2/19 (V).

212 EuGH 4.7.2023, C-252/21 (*Meta u.a./BKartA*) Rz 105 ff, 125, 141 ff, 155.

213 *Müller-Peltzer/Guttmann*, "State of the art" Webtracking, DSB 2023, 233 (233)

214 EDSA 8.10.2019, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gem Art 6 Abs 1 lit b DSGVO iZm der Erbringung von Online-Diensten für betroffene Personen[v2.0], Rz 51 ff, abrufbar unter <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf> (27.4.2024): Selbst dann nicht, wenn ein Online-Dienst finanziell auf Werbeausspielungen zur Erhaltung seines Dienstes angewiesen ist.

215 *Stadler/Bauer/Chochola* in *Bichler* (Hrsg), Praxishandbuch Marketingrecht (2024) 271 ff.

welche mit einer solchen umfangreichen Datenverarbeitung bzw -verknüpfung nicht rechnen mussten (vgl auch Art 5 Abs 2 UAbs 3 DMA). Es komme daher zu erheblichen Auswirkungen auf die Interessen, Grundrechte und Grundfreiheiten der Betroffenen. Im Gegenteil ist für die rechtmäßige Verarbeitung personenbezogener Daten für einen oder mehrere bestimmte Zwecke sowie für die Verarbeitung besonderer Datenkategorien (Art 9 Abs 1 DSGVO) eine wirksame Einwilligung (Art 6 Abs 1 lit a DSGVO) des Betroffenen erforderlich. Eine marktbeherrschende Stellung des Unternehmens kann dabei ein entscheidender Faktor für die Feststellung der Unfreiwilligkeit der Abgabe der Einwilligungserklärung sein (vgl auch ErwGr 42 f DSGVO).[216]

Ferner läuft in Österreich ein bedeutendes Verfahren gegen Facebook,[217] in welchem der OGH[218] den EuGH[219] gleichfalls um die Auslegung wichtiger DSGVO-Bestimmungen gebeten hat.[220] Aufgrund der eben beschriebenen BKartA-Entscheidung des EuGH zog das österreichische Höchstgericht sein Vorabentscheidungsersuchen allerdings tlw zurück,[221] da dessen Vorlagefragen insoweit – va betreffend das Verhältnis zwischen Einwilligung und Vertragserfüllung[222] – beantwortet wurden. Im Endeffekt betrifft das restliche Verfahren vor dem EuGH (nur) noch die Beantwortung der Fragen hinsichtlich eines potenziellen Verstoßes gegen den Grundsatz der Datenminimierung (Art 5 Abs 1 lit c DSGVO) und der Rechtmäßigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten (hier: sexuelle Orientierung), die der Betroffene womöglich selbst „*offensichtlich öffentlich gemacht*" hätte (Art 9 Abs 2 lit e DSGVO). Laut GA *Rantos*[223] macht die öffentliche Äußerung der eigenen sexuellen Orientierung durch den Nutzer eines sozialen Netzwerks dieses Datum zwar offensichtlich öffentlich, doch erlaubt dies nicht dessen Verarbeitung zum Zweck der personalisierten Werbung.

Vor diesem Hintergrund ist es nicht verwunderlich, dass Meta schon im Vorjahr reagierte und eine umfassende Bezahlschranke für die werbefreie Nutzung seiner Online-Dienste

[216] *Thiele*, EuGH: Bundeskartellamt darf DSGVO-Verstöße in Wettbewerbsverfahren prüfen, jusIT 2023/88, 200 (202).
[217] *Kriwanek/Tuma*, Vorlagefragen zur DSGVO und zu personalisierter Werbung, RdW 2021/504, 632 (632 ff).
[218] OGH 23.6.2021, 6 Ob 56/21k.
[219] EuGH laufend, C-446/21 (*Schrems/Facebook*).
[220] *Schmoll*, Rechtmäßigkeit einer Datenverarbeitung, Jus-Extra EuGH 2021, 20 (20).
[221] OGH 19.7.2023, 6 Ob 134/23h.
[222] *Thiele*, Vorlageantrag des OGH: Personalisierte Facebook Werbung, jusIT 2021/90, 241 (243).
[223] GA *Rantos*, SA 25.4.2024, C-446/21 (*Schrems/Facebook*) Rz 49.

einführte.[224] Diese Vorgehensweise sei auch mit der BKartA-Entscheidung vereinbar, denn der EuGH[225] merkte an, dass Nutzern „*gegen ein angemessenes Entgelt, eine gleichwertige Alternative angeboten [werden kann].*" Diese Aussage spiegelt also die bereits von der dt DSK[226] vertretene Ansicht wider, dass „*die Nachverfolgung des Nutzendenverhaltens (Tracking) auf eine Einwilligung gestützt werden [kann], wenn alternativ ein trackingfreies Modell angeboten wird, auch wenn dies bezahlpflichtig ist.*" Hierbei dürfte das entscheidende Merkmal die Marktüblichkeit des Entgelts (grds 5-10 Euro pro Monat) sein.[227]

Es darf jedoch nicht übersehen werden, dass Meta als sog „*Gatekeeper*" an die Bestimmungen des DMA gebunden ist. Es ist ein Fakt, dass solche Torwächter häufig personenbezogene Daten von Endnutzern für Zwecke der Erbringung von Online-Werbediensten erheben und kombinieren, selbst wenn diese Nutzer Internetseiten und Software-Anwendungen Dritter nutzen. Torwächter sollten es Endnutzern aber vielmehr ermöglichen, frei zu entscheiden, ob sie solchen Datenverarbeitungs- und Anmeldungspraktiken zustimmen. Sie sollten eine „*weniger personalisierte, aber gleichwertige Alternative*" anbieten, ohne die Nutzung des zentralen Plattformdienstes oder bestimmter Funktionen von der Einwilligung des Endnutzers abhängig zu machen (ErwGr 36 DMA). Diese weniger personalisierte Alternative sollte sich im Übrigen nicht von dem Dienst unterscheiden, der gegenüber einwilligungserteilenden Endnutzern erbracht wird, oder von geringerer Qualität sein (ErwGr 37 DMA).

Daher leitete die EK[228] eine Untersuchung gegen Meta wegen eines angeblichen Verstoßes gegen Art 5 Abs 2 DMA ein. Dieser schreibt vor, dass Gatekeeper die Zustimmung der Nutzer einholen müssen, wenn sie beabsichtigen, deren personenbezogene Daten über verschiedene zentrale Plattformdienste hinweg zu kombinieren oder zu nutzen. Übrigens wird hiermit auch die Verbindung von Datensätzen zum Training von KI-Systemen unterbunden.[229]

---

[224] *Benedikt/Pfau*, Meta führt im Lichte der EuGH-Entscheidung aus dem Juli 2023 bezahlpflichtiges Abonnement ein, DSB 2024, 6 (6).

[225] EuGH 4.7.2023, C-252/21 (*Meta u.a./BKartA*) Rz 150.

[226] DSK 22.3.2023, Bewertung von Pur-Abo-Modellen auf Websites, Rz 1, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf> (7.4.2024).

[227] *Woerlein*, Personalisierte Werbung und Tracking bei Facebook und Instagram – Abo-Modell statt Datenschutz? ZD-Aktuell 2023, 01467 (beck-online).

[228] EK 25.3.2024, Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act, abrufbar unter <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689> (19.4.2024).

[229] *Hacker*, KI und DMA, GRUR 2022, 1278 (1279).

Gleichfalls gab es Kritik von anderen Stellen: Im bisherigen Verlauf des Jahres forderten nicht nur 39 Abgeordnete des EP[230] Meta in einem offenen Brief zur Einstellung seiner Praktik auf, sondern verlangten auch einige DSB[231] sowie Datenschutz-Vereine[232] eine Stellungnahme des EDSA zu Pay-or-Okay, denn Fakt ist, dass Unternehmen ihre Online-Dienste immer häufiger nach diesem Konzept ausrichten.

2.4.2 EDSA-Stellungnahme zu Pay-or-Okay

Der EDSA[233] stellte ua am 17.4.2024 fest, dass personenbezogene Daten nicht als handelbare Ware betrachtet werden können. Das Grundrecht auf Datenschutz dürfe nicht bloß denjenigen zugutekommen, die für dessen Inanspruchnahme bezahlen. Aus diesem Grund werden die Anforderungen an eine gültige Einwilligung nicht erfüllt, wenn Nutzer vor die Wahl gestellt werden, entweder in die Verarbeitung personenbezogener Daten für verhaltensbezogene Werbung („*Behavioural Advertising*“)[234] einzuwilligen oder eine Gebühr zu zahlen. Eine Freiwilligkeit der Einwilligung ist nicht gegeben, wenn die erhobenen Gebühren so hoch sind, dass sie die betroffenen Personen tatsächlich daran hindern, eine freie Entscheidung zu treffen. Darüber hinaus kann es zu einem gänzlichen Ausschluss vom Zugang kommen, wenn Nutzer ihre Einwilligung verweigern und auch nicht bereit sind, eine Gebühr zu zahlen. Wenn nun zB Facebook oder Instagram – aber etwa auch LinkedIn, TikTok und sonstige VLOPs iSd DSA[235] – eine wichtige Rolle im Leben der Nutzer einnehmen oder für die Teilnahme am gesellschaftlichen Leben oder den Zugang zu beruflichen Netzwerken entscheidend sind (insb wegen

---

[230] *Breyer* 15.3.2024, Offener Brief: Europaabgeordnete fordern Meta zur Abschaffung ihres “Pay or okay”-Modells auf, abrufbar unter <https://www.patrick-breyer.de/offener-brief-europaabgeordnete-fordern-meta-zur-abschaffung-ihres-pay-or-okay-modells-auf> sowie <https://www.patrick-breyer.de/wp-content/uploads/2024/03/MEPs-Letter-to-Meta-on-Pay-or-Okay.pdf> (18.4.2024).

[231] *Etteldorf*, EU: Datenschutzbehörden fordern Stellungnahme des EDSA zu Pay-or-Okay-Modellen, ZD-Aktuell 2024, 01558 (beck-online).

[232] Noyb 16.2.2024, 28 NGOs fordern EU-Behörden zur Ablehnung von „Pay or Okay“ bei Meta auf, abrufbar unter <https://noyb.eu/de/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta> sowie <https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf> (18.4.2024).

[233] EDSA 17.4.2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, abrufbar unter <https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf> (18.4.2024).

[234] Art-29-Datenschutzgruppe 22.6.2010, WP 171, Stellungnahme 2/2010 zur verhaltensbezogenen Werbung, 3 ff, abrufbar unter <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_de.pdf> (18.4.2024).

[235] EK 14.3.2024, Liste der designierten VLOPs und VLOSEs, abrufbar unter <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (18.4.2024).

Netzwerkeffekten),[236] ist es der Ansicht des EDSA zufolge wahrscheinlich, dass Nachteile entstehen, wenn große Online-Plattformen ein „*Consent or Pay*"-Modell verwenden, um die Zustimmung zur Verarbeitung zu erhalten. Demzufolge ist es erforderlich, eine gleichwertige Alternative anzubieten, für die keine Gebühr zu entrichten ist. Dies könnte va eine echte kostenlose Nutzungsmöglichkeit der großen Online-Plattformen sein, die unabhängig von der Verarbeitung personenbezogener Daten für verhaltensbezogene Werbung ist (sog „*Dritte Option*").[237] Eine Finanzierung dieser Online-Dienste könnte nämlich auch anders erfolgen,[238] wie zB über Produktplatzierungen, bezahlte Inhalte oder „*Freemium-Modelle*".[239]

Alles in allem ist diese Stellungnahme mE sehr zu begrüßen, schafft sie doch eine erste wirkliche Orientierungshilfe. Der EDSA merkt jedoch an, dass sich der Untersuchungsumfang ausschließlich auf große Online-Plattformen beschränkt hat. Daher kann nicht mit absoluter Sicherheit davon ausgegangen werden, dass Pay-or-Okay generell unzulässig ist. Die Frage, ob dieses Modell für kleine und mittlere Unternehmen DSGVO-konform ist, wird erst durch Gerichtsentscheidungen geklärt werden müssen. Richtungsweisende Indizien für die Annahme einer Unzulässigkeit könnten bestehende Machtungleichgewichte im Einzelfall zwischen einem Verantwortlichen und den Betroffenen sein.[240] Grds ist einzuräumen, dass va kleine, aufstrebende digitale Plattformen es sich oft nicht leisten können, kostenlos zu sein, weshalb sie auf personalisierte Werbung angewiesen sein könnten. Sie verfügen aller Voraussicht nach (noch) nicht über eine ausreichend große Nutzerbasis, die für ihre Dienste bezahlen würde. Zusammengefasst kann dies dem Wettbewerb schaden und ein Hindernis für den Markteintritt neuer Innovatoren darstellen.[241] Auch das BVwG[242] tendiert in einer zuletzt ergangenen Entscheidung dazu, auf die Marktmacht des Unternehmens abzustellen.

---

[236] Vgl ErwGr 78 DSA.

[237] IAPP 17.4.2024, EDPB opinion on legality of pay-or-consent models in EU GDPR context, abrufbar unter <https://iapp.org/news/a/edpb-opinion-casts-doubt-on-legality-of-pay-or-consent-models-in-eu-gdpr-context> (19.4.2024).

[238] Noyb 17.4.2024, EDSA-Stellungnahme: Meta darf sich nicht auf "Pay or Okay" berufen, abrufbar unter <https://noyb.eu/de/statement-edpb-pay-or-okay-opinion> (18.4.2024).

[239] Freemium-Modelle sind eine Strategie, bei der Unternehmen eine Grund- bzw Basisversion ihres Produkts oder ihrer Dienstleistung kostenlos anbieten („*free*"), während sie zusätzliche Funktionen für zahlende Kunden reservieren („*premium*").

[240] EDSA 17.4.2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 40.

[241] IAPP 16.4.2024, Thoughts on behavioral advertising, Meta and privacy, abrufbar unter <https://iapp.org/news/a/thoughts-on-behavioral-advertising-meta-and-privacy> (19.4.2024).

[242] BVwG 26.4.2024, W211 2281997-1: Zur Freiwilligkeit der Zustimmung zu „unbedingt erforderlichen Marketing- und Analyse-Cookies". Beim Aufruf der Website erschien ein Cookie-Banner, der um die Einwilligung zur

2.5 Nudging & Dark Patterns

Die nachfolgenden Erläuterungen mögen zwar weniger mit Datenschutz per se zu tun haben, dennoch sind sie so eng mit Online-Werbung und KI-Systemen verbunden, dass eine gewisse Analyse im Hinblick auf das Wettbewerbs- und Verbraucherrecht angebracht ist. Ein etwaiger Anknüpfungspunkt im Bereich des Datenschutzrechts ergibt sich aber aus der Frage, ob möglicherweise eine fehlende oder unfreiwillig abgegebene Einwilligung vorliegt.[243] Dies wird idR durch die Nichtbeachtung des Grundsatzes „*Privacy by Design*" (Art 25 Abs 1 DSGVO) begünstigt.[244]

2.5.1 Definition

„*Nudging*"[245] (dt „*Anstupsen*", „*Anstoßen*") bezeichnet eine „*Methode, das Verhalten des Menschen zu beeinflussen, ohne auf Gebote und Verbote zurückzugreifen [und die] auf das Unterbewusste im Menschen zielt, um ein erwünschtes Verhalten zu erreichen.*" Beim „*Digital Nudging*"[246] handelt es sich um das gezielte Ausgestalten von Benutzeroberflächen, sei es auf Websites, in Apps oder anderen Anwendungen, mit dem Ziel, das Entscheidungsverhalten von Nutzern zu beeinflussen. Dies erfolgt durch verschiedene Designmerkmale wie Texte, Farbwahl, audiovisuelle Elemente wie Töne und Videos, Erinnerungen, Push-Benachrichtigungen und Rückmeldungen, sowie durch das Formulieren von Inhalten und deren Anordnung.[247]

Verarbeitung von personenbezogenen Daten ersuchte. Nach Verweigerung der Zustimmung zu jeglichen Verarbeitungsvorgängen durch die entsprechende Auswahl im Untermenü „Einstellungen verwalten" und deren Bestätigung erschien jedoch ein weiteres „Pop-up"-Fenster (sog „*Double-Layer*"). Dieses wies auf die unbedingte Erforderlichkeit der Dienste „Google Advertising Products", „Google Tag Manager", „Google Analytics" und „ÖWA" hin. Ein Besuch der Website des Unternehmens ohne Zustimmung zu den genannten Diensten war nicht möglich. Das BVwG bestätigte – im Gegensatz zum erstinstanzlichen Bescheid der DSB – in diesem Fall die Freiwilligkeit, wenn die Website trotzdem besucht wird. Ob dieses Urteil vor dem VwGH Bestand haben wird, ist derzeit unklar. Da das Unternehmen mittlerweile selbst auf ein (noch) datenschutzkonformes Pay-or-Okay-Konzept umgestellt hat, ist mE anzunehmen, dass das BVwG-Urteil erhebliche Rechtsunsicherheiten aufwirft und die Freiwilligkeit im Ausgangsfall eher doch zu verneinen ist.

[243] Vgl Kapitel 2.1 (Tracking & Cookies): Es sind idR Cookie-Banner, die farblich und technisch so konzipiert sind, um Besucher einer Webseite dazu zu bewegen, ihre Zustimmung zu geben.

[244] DSK 3.4.2019, Hambacher Erklärung zur Künstlichen Intelligenz, 2, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf> (20.4.2024).

[245] *Hufen*, Nudging, JuS 2020, 193 (193 f).

[246] *Kammerl/Kramer/Müller/Potzel/Tischer/Wartberg*, Dark Patterns und Digital Nudging in Social Media - wie erschweren Plattformen ein selbstbestimmtes Medienhandeln? BLM-Schriftenreihe 110 (2023) 40 ff.

[247] *Machnik/Gross* 16.3.2022, Die dunkle Seite von Digitalem Nudging, abrufbar unter <https://www.uibk.ac.at/ibf/blog-wirtschaft-und-verantwortung/posts/die-dunkle-seite-von-digitalem-nudging.html> (19.4.2024).

Hierbei werden diverse psychologische Prinzipien eingesetzt, um spezifische Reaktionen bei der Zielgruppe hervorzurufen.[248] Es steht außer Frage, dass bedenkliche Formen der indirekten Beeinflussung im Bereich der Werbung[249] existieren, bei denen Menschen bereit sind, ihre Selbstbestimmung und den Schutz ihrer persönlichsten Daten zugunsten realer oder vermeintlicher Vorteile aufzugeben.

Die genaue Abgrenzung zu „*Dark Patterns*"[250] (dt „*Dunkle Muster*") ist nicht gänzlich gelöst, wobei letzteres eher als Sammelbegriff gilt,[251] weil sie nicht nur menschliches Verhalten lenken, sondern vielmehr missbräuchlich wirken. Deshalb kursiert auch der Begriff des „*Dark Nudging*",[252] der sich auf die Intransparenz solcher täuschenden und manipulativen Praktiken bezieht. Dark Patterns verleiten Nutzer geschickt zu bestimmten Aktionen, während Nudging sie sanft (ohne Zwang) zu den gewünschten Ergebnissen führt.

Der EDSA[253] differenziert zwischen 6 Kategorien von sog „*irreführenden Gestaltungsmustern*". Ihr Ziel ist jedoch identisch: es sollen mehr Vertragsabschlüsse oder -verlängerungen generiert, höhere Interaktionsraten erreicht oder mehr Daten gesammelt werden, die letztendlich durch Werbung monetarisiert werden können.[254] Die Arbeiterkammer Wien[255] hat sich diesem Problem ebenfalls gewidmet und in einer Studie einige ernste Anwendungsfälle aufgezeigt.

---

[248] Im Bereich der sog „*Free-to-Play*"-Spiele werden hauptsächlich junge Spieler dazu ermutigt, mit echtem Geld sog „*Loot-Boxen*" zu kaufen, um ihre Spielfiguren mit exklusiven Skins oder anderen seltenen Gegenständen auszustatten. Es gibt auch zunehmend Vorwürfe gegen diese „*Pay-to-Win*"-Konzepte, bei welchen Spieler durch den Kauf von Inhalten einen unfairen Vorteil erlangen können, was mit echtem Glücksspiel assoziiert wird. Spieler geben oft große Geldsummen aus, um das gewünschte Objekt schließlich durch „Zufall" zu erhalten.

[249] Man denke insb an Knappheits-Meldungen, welche Verbrauchern auf Online-Plattformen Countdowns und ähnliche „Warnhinweise" – wie zB „*Nur noch 5 Zimmer zu diesem Preis*" – anzeigen, um Druck aufzubauen; vgl *Martini/Kramme/Seeliger*, „Nur noch für 30 Minuten verfügbar" – Scarcity- und Countdown-Patterns bei Online-Geschäften auf dem Prüfstand des Rechts, VuR 2022, 123 (123).

[250] *Gertz/Martini/Seeliger/Timko*, Dark Patterns - eine interdisziplinäre Analyse, LTZ 2023, 3 (3).

[251] *Martini/Drews/Seeliger/Weinzierl*, Dark Patterns, ZfDR 2021, 47 (49).

[252] *Kammerl/Kramer/Müller/Potzel/Tischer/Wartberg*, Dark Patterns und Digital Nudging in Social Media - wie erschweren Plattformen ein selbstbestimmtes Medienhandeln? BLM-Schriftenreihe 110 (2023) 52.

[253] EDSA 14.2.2023, Leitlinien 03/2022 zu irreführenden Gestaltungsmustern in Schnittstellen von Social-Media-Plattformen: Wie man sie erkennt und vermeidet$^{v2.0}$, 3 f, abrufbar unter <https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf> (9.5.2024).

[254] *Martini/Drews/Seeliger/Weinzierl*, Dark Patterns, ZfDR 2021, 47 (53).

[255] Arbeiterkammer Wien März 2023, Verlorene Zeit, Verlorenes Geld – Dark Patterns im Alltag von Konsument:innen, abrufbar unter <https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/Internet/Dark_Patterns.pdf> (19.4.2024).

Insgesamt können KI-basierte Algorithmen bereits jetzt die Möglichkeiten zur (mikrogezielten) Manipulation von Benutzerverhalten erheblich verstärken.[256] Da digitale Benutzeroberflächen immer flexibler und individuell in Echtzeit angepasst werden können, spricht man nun auch vom sog „*Hypernudging*".[257] Algorithmen im Marketing unterscheiden grds nicht eigenständig zwischen realisierten Umsätzen von getäuschten und nicht getäuschten Verbrauchern. Eine rein auf Umsatzmaximierung ausgelegte KI erkennt daher zB nicht, ob ein Verbraucher betrunken war und unter einem falschen Eindruck stand, der für die Transaktion wesentlich war, weil das System nur Umsätze misst. *Willis*[258] geht in solchen Fällen sogar davon aus, dass die Technologie zwangsläufig täuschen wird, um die Umsätze zu steigern. *Lorenz*[259] weist darauf hin, dass automatisierte, unkontrollierte Marketingäußerungen dazu führen können, dass Verbraucher irreführende Informationen erhalten. Dies unterstreicht erneut die Notwendigkeit einer ethischen Nutzung von KI-Technologien und einer kritischen Reflexion über die Auswirkungen auf die Privatsphäre und Autonomie der Verbraucher iZm datengesteuerten Personalisierungspraktiken.

Abseits der KI-VO werden solche Verhaltensweisen schon im Rahmen der europäischen Digitalstrategie behandelt,[260] auf welche im Folgenden eingegangen wird.

2.5.2 Regulierung durch den DSA

Der DSA definiert Dark Patterns als „*Praktiken, mit der darauf abgezielt oder tatsächlich erreicht wird, dass die Fähigkeit der Nutzer, eine autonome und informierte Auswahl oder Entscheidung zu treffen, maßgeblich verzerrt oder beeinträchtigt wird*" (ErwGr 67 DSA).[261]

---

[256] *Prange*, Datenschutz- und lauterkeitsrechtliche Kernfragen des Einsatzes Künstlicher Intelligenz im Marketing, WRP 2024, 151 (Rz 36 f).

[257] *Yeung*, 'Hypernudge': Big Data as a mode of regulation by design, Information Communication and Society (2016) 6, abrufbar unter <https://www.researchgate.net/publication/303479231_'Hypernudge'_Big_Data_as_a_mode_of_regulation_by_design> (20.4.2024).

[258] *Willis*, Deception by Design, Harvard Journal of Law & Technology[vol.34] Number 1 Fall 2020, 148, abrufbar unter <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694575> (20.4.2024).

[259] *Lorenz*, Chatbots im praktischen Einsatz: Grundbegriffe, Rechtsfragen und Anwendungsszenarien, KuR 2019, 1 (5 ff).

[260] *Weinzierl*, Neue Dark-Patterns-Verbote als Abschied vom homo oeconomicus im EU-Recht, EuZW 2024, 345 (346).

[261] *Nemec*, Digital Services Act und Verbraucherschutz, ecolex 2024/119, 219 (219).

Anbieter von Online-Plattformen[262] dürfen ihre Online-Schnittstellen[263] dementsprechend nicht so konzipieren, organisieren oder betreiben, dass Nutzer[264] getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, eine freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden (Art 25 Abs 1 DSA). Dies kann entweder bewusst iSv absichtlich und böswillig („*abzielen*") oder durch erhebliche Entscheidungsverzerrungen bzw -beeinträchtigungen, die zu gewünschten Verhaltenseffekten führen („*tatsächlich erreichen*") stattfinden.[265] Allerdings wird – ähnlich wie in ErwGr 29 KI-VO – hervorgehoben, dass „*rechtmäßige Praktiken – beispielsweise in der Werbung –, die mit dem Unionsrecht im Einklang stehen, an sich nicht als Dark Patterns angesehen werden [sollten].*"

Die Vorschriften des DSA über verbotene Dark Patterns gelten insoweit nur, wenn eine Geschäftspraxis nicht schon durch die UGP-RL[266] und die DSGVO erfasst wird (Art 25 Abs 2 DSA). Zur besseren Orientierung erlies die EK[267] einschlägige Leitlinien, in welchen ua angemerkt wird, dass die „*UGP-RL die Phasen der Werbung, des Verkaufs und der Vertragserfüllung [abdeckt], einschließlich der Einwilligung zur Verarbeitung personenbezogener Daten und der Verwendung personenbezogener Daten für die Bereitstellung personalisierter Inhalte sowie der Beendigung eines Vertragsverhältnisses*". Die EK betrachtet die UGP-RL gemeinsam mit der ePrivacy-RL und der DSGVO als Instrumente zur Bekämpfung unlauterer datengesteuerter Geschäftspraktiken zwischen Unternehmen und Verbrauchern. Diese Sichtweise gründet sie explizit auf die Tatsache, dass das digitale Umfeld zunehmend von der Generierung, Sammlung und Kontrolle großer Datenmengen über Verbraucher geprägt ist. Diese Daten können durch den Einsatz von Algorithmen und KI kombiniert werden, um sie in verwertbare Informationen für kommerzielle Zwecke umzuwandeln.

---

[262] Das sind (nur) Hostingdienste, die im Auftrag eines Nutzers Informationen speichern und öffentlich verbreiten (Art 3 lit i DSA). ErwGr 13 DSA zählt dazu zB Social-Media-Plattformen oder E-Commerce-Plattformen (Online-Marktplätze). Somit fallen nicht sämtliche Vermittlungsdienste (Art 3 lit g) unter das Dark Pattern-Verbot.

[263] Das ist grds jede Software, ua Webseiten und Apps (Art 3 lit m DSA).

[264] Das ist jede natürliche oder juristische Person, die einen Vermittlungsdienst in Anspruch nimmt (Art 3 lit b DSA). Art 25 DSA schützt also auch im B2B-Bereich (vgl auch ErwGr 2 DSA).

[265] *Gerpott*, Bekämpfung von Dark Patterns auf Nutzerschnittstellen mittels neuer EU-Rechtsakte für den digitalen Raum, KuR 2022, 726 (726).

[266] RL 2005/29/EG, ABl 2005/L 149, 22, zuletzt geändert durch RL (EU) 2019/2161, ABl 2019/L 328, 7. Die UGP-RL bewirkt eine Vollharmonisierung im B2C-Bereich und wurde in Österreich vollständig im UWG, BGBl Nr 448/1984 idF BGBl I Nr 99/2023, umgesetzt; vgl *Falke/Pachschwöll* in *Bichler* (Hrsg), Praxishandbuch Marketingrecht (2024) 171 ff.

[267] EK 29.12.2021, Leitlinien zur Auslegung und Anwendung der RL 2005/29/EG, ABl 2021/C 526, 1 (99 ff).

Da nahezu jede Online-Aktivität die Verarbeitung personenbezogener Daten beinhaltet, würde Art 25 DSA ins Leere laufen, sobald die DSGVO anwendbar wäre.[268] Art 25 Abs 2 DSA ist jedoch so zu interpretieren, dass Praktiken, die bereits nach der DSGVO bzw UGP-RL verboten sind, nach dem jeweiligen Regelwerk behandelt werden sollen.[269] Die Beurteilung einer datenschutzkonformen Einwilligung richtet sich daher zB (nur) nach der DSGVO. Hingegen werden Dark Patterns, die als aggressive oder irreführende geschäftliche Handlungen eingestuft werden, weiterhin nach den Prinzipien des Wettbewerbsrechts beurteilt. Art 25 DSA hat immerhin einen autonomen Anwendungsbereich, insb im Hinblick auf die Verarbeitung nichtpersonenbezogener Daten, inkl der Daten juristischer Personen.[270]

Neben dem Thema Dark Patterns enthält der DSA Regelungen, die für das Online-Marketing von großer Bedeutung sind.[271] Einige der wichtigsten Implikationen sollen daher kurz erläutert werden. „*Werbung*" iSd DSA sind alle „*Informationen, die dazu bestimmt sind, die Botschaft einer juristischen oder natürlichen Person zu verbreiten, unabhängig davon, ob damit gewerbliche oder nichtgewerbliche Zwecke verfolgt werden, und die von einer Online-Plattform auf ihrer Online-Schnittstelle gegen Entgelt speziell zur Bekanntmachung dieser Informationen dargestellt werde*n" (Art 3 lit r DSA). Der DSA gilt sohin für jede Art von Werbung, vom digitalen Marketing über themenbezogene Werbung bis hin zu politischen Anzeigen.[272] Online-Werbung kann trotz allem erhebliche Risiken bergen (ErwGr 68 DSA).[273] Dies wird ua der Fall sein, wenn die Werbung selbst rechtswidrige Inhalte aufweist oder wenn Nutzern Werbung angezeigt wird, die auf Techniken der Personalisierung beruht, welche optimiert sind, um ihren Interessen zu entsprechen und möglicherweise auf ihre Schwächen abzielen (ErwGr 69 DSA).

Im Besonderen kann die Gestaltung der Dienste von VLOPs und VLOSEs gesellschaftliche Bedenken hervorrufen, da sie idR darauf ausgelegt sind, ein oft werbegestütztes Geschäftsmodell[274] zu optimieren (ErwGr 79 DSA). Darum müssen bei der Bewertung der systematischen

[268] *Dregelies*, Der Schutz vor Dark Patterns im DSA, MMR 2023, 243 (246 f).
[269] *Blümel*, Dark Patterns im DSA und DMA: unzulässige digitale Beeinflussung von Entscheidungsprozessen, ecolex 2023/567, 896 (896).
[270] *Raue* in *Hofmann/Raue* (Hrsg), Digital Services Act (2023) Art 25 Rz 100, 102.
[271] *Wolfbauer/Demschik*, Datenverarbeitung im Zeitalter des Metaverse, ecolex 2022/348, 512 (512).
[272] EK 23.2.2024, Questions and answers on the Digital Services Act, abrufbar unter <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> (20.4.2024).
[273] *Janal*, Haftung und Verantwortung im Entwurf des Digital Services Acts, ZEuP 2021, 227 (268).
[274] Vgl Kapitel 2.4 (Pay-or-Okay).

Risiken derartiger Vermittlungsdienste die tatsächlichen oder absehbaren Auswirkungen auf die Grundrechte einkalkuliert werden, weil diese Risiken uU auf die Gestaltung der algorithmischen Systeme, Empfehlungssysteme[275] und Werbesysteme zurückzuführen sind (ErwGr 81, 84 DSA). Werbesysteme können auch ein Katalysator für systemische Risiken sein (ErwGr 88 DSA), sodass VLOPs und VLOSEs evtl angehalten sind, ihre algorithmischen Systeme und Empfehlungssysteme zu testen und erforderlichenfalls anzupassen, insb wenn eine derartige Anpassung im Einklang mit dem Datenschutzrecht steht (vgl ErwGr 94 DSA). Zusätzlich müssen sie die negativen Auswirkungen personalisierter Empfehlungen mindern, die in ihren Empfehlungen verwendeten Kriterien korrigieren und Werbearchive[276] öffentlich zugänglich machen (ErwGr 95 DSA).

In Anbetracht dessen unterscheidet der DSA im Folgenden zwischen Informationspflichten und konkreten Werbeverboten.[277] Anbieter von Online-Plattformen, die Werbung auf ihren Online-Schnittstellen schalten, müssen zunächst sicherstellen, dass Nutzer jeder einzelnen Werbung in klarer, präziser und eindeutiger Weise und in Echtzeit entnehmen können, (i) dass es sich um Werbung handelt, (ii) wer die natürliche oder juristische Person ist, in deren Namen die Werbung angezeigt wird, und (iii) wer die natürliche oder juristische Person ist, die für die Werbung bezahlt hat. Es müssen auch aussagekräftige Informationen über die wichtigsten Parameter zur Bestimmung der Nutzer, denen die Werbung angezeigt wird, vorhanden sein und darüber, wie diese Parameter uU geändert werden können (Art 26 Abs 1 DSA).[278] Dieses „*Transparenzgebot*"[279] wird durch die E-Commerce-RL[280] ergänzt und sollte auch Aussagen über die für die Anzeige der Werbung verwendete Methode (zB kontextbezogene Werbung) sowie gegebenenfalls die wichtigsten verwendeten Profiling-Kriterien enthalten (vgl ErwGr 68,

[275] Das ist ein vollständig oder teilweise automatisiertes System, das von einer Online-Plattform verwendet wird, um Nutzern auf ihrer Online-Schnittstelle bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren, auch infolge einer vom Nutzer veranlassten Suche, oder das auf andere Weise die relative Reihenfolge oder Hervorhebung der angezeigten Informationen bestimmt (Art 3 lit s DSA). Dies geschieht zB durch algorithmische Empfehlungen, Einstufung und Priorisierung von Informationen, die durch textliche oder andere visuelle Darstellungen kenntlich gemacht werden, oder durch andere Arten der Kuratierung der von Nutzern bereitgestellten Informationen (ErwGr 70 DSA).

[276] EuGH 27.3.2024, C-639/23 P(R) (*EK/Amazon*) Rz 176: Das Gericht wies den Antrag von Amazon auf Aussetzung seiner Pflicht, ein Werbearchiv öffentlich zugänglich zu machen, ab.

[277] *Bichler*, Digital Services Act und Online Marketing, ecolex 2024/120, 222 (222).

[278] *Stadler/Drolz* in *Bichler* (Hrsg), Praxishandbuch Marketingrecht (2024) 446 ff.

[279] *Grisse* in *Hofmann/Raue* (Hrsg), Digital Services Act (2023) Art 26 Rz 17 ff.

[280] RL 2000/31/EG, ABl 2000/ L 178, 1, welche in Österreich im ECG, BGBl I Nr 152/2001 idF BGBl I Nr 182/2023, umgesetzt wurde.

69 DSA). Außerdem gelten diese Bestimmungen unabhängig von der ePrivacy-RL und DSGVO, wonach vor der Verarbeitung personenbezogener Daten für gezielte Werbung die Einwilligung der betroffenen Person einzuholen ist. Werden Empfehlungssysteme (zB „*Das könnte Ihnen auch gefallen*") eingesetzt, müssen Online-Plattformanbieter zusätzliche Transparenzpflichten einhalten (Art 27 DSA).[281] Sog „*Filterblasen*"[282] gilt es absolut zu vermeiden, in der Menschen nur Informationen sehen, die ihre bestehenden Überzeugungen bestätigen, was die Vielfalt der Meinungen einschränken kann.

Zu den spezifischen „*Werbeverboten*" gehören: (a) das Verbot, volljährigen Nutzern Werbung anzuzeigen, sofern diese auf Profiling unter Verwendung besonderer Kategorien personenbezogener Daten beruht (Art 26 Abs 3 DSA),[283] und (b) das Verbot, Minderjährigen profilingbasierte Werbung anzuzeigen, unabhängig davon, ob im Zuge des Profiling sensible Daten verarbeitet wurden oder nicht (Art 28 Abs 2 DSA; vgl auch ErwGr 71 DSA).[284] Aus diesem Grund ist es für Anbieter von Online-Plattformen ratsam, das Alter ihrer (potenziellen) Nutzer vorab zu kontrollieren. Eine Pflicht, zusätzliche personenbezogene Daten zu verarbeiten, um eine etwaige Minderjährigkeit der Nutzer festzustellen, besteht aber nicht (Art 28 Abs 3 DSA). Problematisch ist mE, dass Kleinst- und Kleinunternehmen[285] grds nicht unter diese Gebote und Verbote des DSA fallen (Art 19 DSA). Werbespezifische Sonderregeln existieren dafür für VLOPs und VLOSEs. Hier sind va die Pflicht zum Anbieten mind eines Empfehlungssystems ohne Profiling (Art 38 DSA)[286] und die Werbearchive (Art 39 DSA)[287] zu nennen.

Neulich unterzeichneten die RTR-GmbH, KommAustria und die DSB ein MoU iSe Kooperationsvereinbarung, in welcher sich die Behörden zu einer Abstimmung über datenschutzrelevante Bestimmungen des DSA verpflichten.[288] Eine bedeutende Schnittstelle zwischen KI und dem DSA ist das Europäische Zentrum für die Transparenz der Algorithmen (ECAT), das 2023

[281] *Grisse* in *Hofmann/Raue* (Hrsg), Digital Services Act (2023) Art 27 Rz 8.
[282] *Schwartmann/Hermann/Mühlenbeck*, Eine Medienordnung für Intermediäre, MMR 2019, 498 (503).
[283] *Schmieke* in *Gerecke* (Hrsg), Handbuch Social-Media-Recht (2023) Kap 3 Rz 75.
[284] Kinder verdienen Sonderschutz bzgl ihrer personenbezogenen Daten, insb im Hinblick auf die Verwendung für Zwecke kommerzieller Kommunikation oder der Erstellung von Nutzerprofilen (ErwGr 38 DMA).
[285] EK 6.5.2003, Empfehlung betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl 2003/L 124, 36 (38).
[286] *Maamar* in *Kraul* (Hrsg), Das neue Recht der digitalen Dienste (2023) § 4 Rz 232 ff.
[287] *Grisse* in *Hofmann/Raue* (Hrsg), Digital Services Act (2023) Art 39 Rz 2.
[288] RTR 23.4.2024, Zusammenarbeit im Zeichen des DSA: Datenschutzbehörde, KommAustria und RTR-GmbH definieren Kooperation, abrufbar unter <https://www.rtr.at/medien/presse/pressemitteilungen/Presseinformationen_2024/PI04232024RTRM_MoU_DSB_KOA_RTR.html> (25.4.2024).

eingerichtet wurde. Das ECAT stellt wissenschaftliches und technisches Fachwissen zur Verfügung, um die Umsetzung des DSA zu unterstützen und die Effekte algorithmischer Systeme zu erforschen, die von (sehr großen) Online-Plattformen und Suchmaschinen genutzt werden.[289]

Weil solche Systeme Informationen identifizieren, kategorisieren, bewerten, vorschlagen und präsentieren sowie menschliche Entscheidungen unterstützen, beeinflussen oder sogar oft ersetzen, hat die EK[290] eine Strategie vorgelegt, die darauf abzielt, „*KI-Exzellenz*" in Europa zu fördern, sicherzustellen, dass KI-Systeme vertrauenswürdig[291] sind und die Sicherheit sowie die Grundrechte der europäischen Bürger zu schützen.

2.5.3 Regulierung durch den DMA

Gem ErwGr 14 DMA können Online-Werbedienste, einschließlich Werbenetzwerke, Werbebörsen und sonstige Werbevermittlungsdienste, Auswirkungen auf viele Endnutzer und Unternehmen haben. Dies birgt das Risiko, dass „*unfaire Geschäftspraktiken*" angewendet werden.[292] Daher fallen diese Dienste ebenfalls unter den Begriff der „*zentralen Plattformdienste*" (Art 2 Z 2 lit j DMA), die von designierten „*Torwächtern*" (Gatekeeper)[293] bereitgestellt werden (Art 2 Z 1 DMA iVm Art 3 DMA).[294]

Werberechtliche Besonderheiten finden sich im DMA ua an folgenden Stellen: Zunächst dürfen Torwächter ihre Online-Schnittstellen nicht so gestalten, organisieren oder betreiben, dass Endnutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, ihre Einwilligung iSd DSGVO frei zu erteilen, maßgeblich beeinträchtigt oder behindert werden (ErwGr 37 DMA).

---

[289] ECAT, About ECAT, abrufbar unter <https://algorithmic-transparency.ec.europa.eu/about_en> (22.4.2024).

[290] EK, Trustworthy AI, abrufbar unter <https://ai-watch.ec.europa.eu/topics/trustworthy-ai_en> (22.4.2024); EK 24.2.2023, JRC portfolio 15: Trustworthy AI, abrufbar unter <https://joint-research-centre.ec.europa.eu/jrc-science-and-knowledge-activities/trustworthy-artificial-intelligence-ai_en> (22.4.2024).

[291] Vgl ErwGr 27 KI-VO und die Hochrangige Expertengruppe für Künstliche Intelligenz 8.4.2019, Ethik-Leitlinien für eine vertrauenswürdige KI, abrufbar unter <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (22.4.2024); vgl OECD 3.5.2024, Principles for trustworthy AI, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, abrufbar unter <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (9.5.2024).

[292] Vorausgeschickt wird, dass der DMA unbeschadet anderer EU-Rechtsakte, darunter die DSGVO, die UGP-RL und die ePrivacy-RL, gilt (ErwGr 12 DMA).

[293] Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta (Facebook) und Microsoft. Unter den Online-Werbediensten sind aber nur Google, Amazon und Meta aufgeführt; vgl EK 5.9.2023, Ernennungsbeschlüsse, abrufbar unter <https://digital-markets-act.ec.europa.eu/gatekeepers_en> (22.4.2024).

[294] *Lettl*, Das Gesetz über digitale Märkte (Digital Markets Act - DMA), WRP 2022, 1453 (Rz 13 ff).

Darüber hinaus ist es unzulässig, Endnutzer mehr als einmal jährlich aufzufordern, eine Einwilligung für denselben Verarbeitungszweck zu erteilen, für den diese ursprünglich keine Einwilligung erteilt oder ihre Einwilligung widerrufen haben (vgl auch Art 5 Abs 2 DMA).[295] Hinzukommend regeln DMA und DSA partiell dieselben Aspekte: Während im DSA von Empfehlungssystemen die Rede ist, verwendet der DMA den Begriff „*Ranking*" (Art 2 Z 22 DMA, ErwGr 51 f, 61 DMA).[296] Hierdurch wird die öfters anzutreffende P2B-Komponente[297] des DMA hervorgehoben (Art 6 Abs 5 DMA: rankingbezogene Transparenzpflicht und Selbstbevorzugungsverbot bzgl Ranking).[298] Des Weiteren sollen Informationspflichten gegenüber Werbetreibenden und Herausgebern (Art 5 Abs 9-10 DMA)[299] es diesen ermöglichen, die Kennzahlen zu erfahren, anhand derer die einzelnen Preise, Gebühren und Vergütungen für vermittelte Werbung berechnet werden (vgl ErwGr 45 ff DMA).[300] Die offengelegten Angaben dürfen jedoch nicht die datenschutzrechtlich geschützten Belange der Endnutzer beeinträchtigen.[301]

Dennoch ist ein wesentlicher KI-Bezug erkennbar: Weil die Kennzahlen – worunter auch Algorithmen zu verstehen sind – preisgegeben werden müssen, sind die Gatekeeper nunmehr verpflichtet, erklärungsfähige KI-Systeme zu verwenden, damit die individuelle Entscheidung für jede einzelne Werbung anhand der Entscheidungsfaktoren nachvollziehbar ist.[302] Art 6 Abs 8 DMA sieht ähnliche Bestimmungen für die von Gatekeepern verwendeten Leistungsmessinstrumente vor (vgl ErwGr 58 DMA).[303] Dies betrifft ua die Vorhersagegenauigkeit von KI-Systemen und die Konversionsraten („*Click Through Rate*") von Werbeanzeigen.[304] Konkrete Rechte (Art 6 Abs 10-11 DMA)[305] sollen bestimmten Akteuren überdies Zugang zu (anonymisierten personenbezogenen) Nutzungsdaten[306] und Suchdaten (Ranking-, Anfrage-, Klick- und Ansichtsdaten) unter sog „*FRAND*"-Konditionen[307] geben. Der Datenzugang soll

[295] Vgl Kapitel 2.4.1 (Pay-or-Okay).
[296] *Pfeiffer/Helmke*, Die Digitalrechtsakte der EU (DGA, DSA, DMA, KI-VO-E und DA-E) – Teil I, ZD-Aktuell 2023, 01125 (beck-online).
[297] Vgl P2B-VO (EU) 2019/1150, ABl 2019/L 186, 57.
[298] *Heinz* in *Podszun* (Hrsg), Digital Markets Act (2023) Art 6 Rz 83 ff.
[299] *Louven* in *Gersdorf/Paal* (Hrsg), BeckOK Informations- und Medienrecht[43.EL] (2023) Art 5 Rz 116 ff.
[300] *Herbers/Savary*, Der Digital Markets Act kommt, CB 2022, 196 (196).
[301] *Bueren/Weck* in *Säcker* (Hrsg), Münchener Kommentar zum Wettbewerbsrecht 1/1[4] (2023) Art 5 Rz 247.
[302] *Hacker*, KI und DMA, GRUR 2022, 1278 (1279).
[303] *Gasser/Hegener* in *Schmidt/Hübener* (Hrsg), New Digital Markets Act (2023) Kap 6 Rz 69 ff.
[304] *Hacker*, KI und DMA, GRUR 2022, 1278 (1279).
[305] *Gasser/Hegener* in *Schmidt/Hübener* (Hrsg), Das neue Recht der digitalen Märkte (2023) § 6 Rz 76 ff.
[306] Endnutzer müssen allerdings in eine solche Weitergabe einwilligen (ErwGr 60 DMA).
[307] „*Fair, Reasonable And Non-Discriminatory*" (dt „*fair, angemessen und nicht-diskriminierend*").

Wettbewerbern des Torwächters garantieren, ihre eigenen Dienste (KI-Systeme) durch das Training mit den bereitgestellten Daten zu verbessern und so ihre Marktposition zu stärken (ErwGr 61 DMA).[308] Bemerkenswert ist auch das Umgehungsverbot des Art 13 Abs 4 DMA, wonach ein Torwächter *„kein Verhalten an den Tag legen [darf], das die wirksame Einhaltung der Verpflichtungen aus den Art 5, 6 und 7 untergräbt.*" Der DMA nennt in diesem Zusammenhang *„Verhaltenslenkungsmethoden"* als unerwünschte Praktiken, die Techniken wie Nudging und Dark Patterns umfassen.[309]

Die Transparenzregeln des DSA und DMA streben letztendlich danach, einen Teil des Rätsels um die KI-Blackbox zu lüften, indem sie Gatekeeper dazu auffordern, verständliche KI-Systeme[310] zu nutzen und den Zugang zu wesentlichen Daten und Metriken zu ermöglichen.[311] Es wird eine beträchtliche Investition an Zeit und Aufwand erfordern, um die volle Tragweite dieser Regelungen zu verstehen und sowohl den Adressaten der Normen als auch der Gesellschaft insgesamt zu verdeutlichen, dass es sich dabei nicht um bloße bürokratische Vorgaben aus Brüssel handelt, sondern um einen echten Versuch, die Nutzung von KI und Datenwirtschaft in Europa grundrechtskonform zu gestalten.[312]

2.5.4 Regulierung durch den DA

Vorab muss explizit festgehalten werden, dass der DA kein neues Recht für Dateninhaber[313] auf die Erhebung und Nutzung von Daten verleiht, die bei der Nutzung eines *„vernetzten Produkts*" (*„IoT-Gerät*")[314] oder *„verbundenen Dienstes*"[315] generiert werden (ErwGr 5 DA). Das gilt natürlich auch für sog *„Virtuelle Assistenten*".[316]

---

[308] *Polley/Konrad*, Der Digital Markets Act – Brüssels neues Regulierungskonzept für Digitale Märkte, WuW 2021, 198 (204).

[309] *Bueren/Weck* in *Säcker* (Hrsg), Münchener Kommentar zum Wettbewerbsrecht 1/1[4] (2023) Art 13 Rz 25.

[310] Vgl OECD, Catalogue of Tools & Metrics for Trustworthy AI, abrufbar unter <https://oecd.ai/en/catalogue/overview> (25.4.2024): Dieser Katalog soll KI-Akteuren helfen, vertrauenswürdige KI-Systeme zu entwickeln und zu nutzen, die die Menschenrechte achten sowie fair, transparent, erklärbar, robust, sicher und geschützt sind.

[311] *Kruesz*, Die Regulierung des Einsatzes von Algorithmen in der DS-GVO, im E-DSA und E-DMA: Hält dreifach wirklich besser? jusIT 2021/1, 1 (7).

[312] *Staudegger*, Aktuelles aus dem IT-Recht - Daten-Governance-Rechtsakt (DGA), Gesetz über Digitale Märkte (DMA), Gesetz über Digitale Dienste (DSA), jusIT 2023/40, 85 (92).

[313] Art 2 Z 13 DA; ErwGr 25, 63 DA.

[314] Art 2 Z 5 DA; ErwGr 14 DA: zB Smart Home-Geräte.

[315] Art 2 Z 6 DA; ErwGr 17 DA: zB Smartwatch, die zusätzlich Gesundheitsdaten misst (ua den Schlafrhythmus).

[316] Art 2 Z 31 DA; ErwGr 23 DA: zB Voicebots (ua Alexa, Siri, Cortana, Google Assistent) und Chatbots.

Es wird darauf aufmerksam gemacht, dass jegliche Verarbeitung personenbezogener Daten dem europäischen Datenschutzrecht entsprechen muss, einschließlich des Erfordernisses einer gültigen Rechtsgrundlage für die Datenverarbeitung iSd DSGVO (Art 1 Abs 5 DA, ErwGr 7 DA). Nutzer[317] sollen auf der anderen Seite fortan das Recht haben, nicht-personenbezogene Daten[318] zu kommerziellen und nichtkommerziellen Zwecken an Datenempfänger[319] weiterzugeben (ErwGr 26 DA). Nach Zustimmung des Nutzers sollten Dritte die vom Nutzer eingeräumten Datenzugangsrechte[320] (entgeltlich) auf andere Dritte übertragen dürfen (ErwGr 33 DA). Die Idee ist, dass die Nutzer durch neu erworbene Zugriffsrechte zu einer besseren Datenverfügbarkeit beitragen, indem sie Datensilos, insb die der Gerätehersteller, dezentral aufbrechen.[321] Dies könnte eine „*entscheidende Rolle bei der Aggregation des Zugangs zu Daten spielen, sodass Big Data-Analysen oder maschinelles Lernen erleichtert werden können, vorausgesetzt dass die Nutzer die volle Kontrolle darüber behalten, ob sie ihre Daten zu einer solchen Aggregation bereitstellen und unter welchen kommerziellen Bedingungen ihre Daten zu nutzen sind*“ (vgl auch ErwGr 34 DA).[322]

Möglicherweise übersehen wurde, dass sich ein Zugangsanspruch immer nur auf die vom jeweiligen Nutzer selbst generierten Daten und nicht auch auf Daten anderer Nutzer bezieht.[323] Die Datenzugangs- und -nutzungsregeln der Art 3 ff DA[324] scheinen demnach für die Entwicklung und das Training von KI-Systemen, die auf aggregierten Daten einer Vielzahl von Nutzern basieren, de facto unzureichend zu sein.[325] Aus datenschutzrechtlicher Perspektive ist dem zuzustimmen, denn schon jetzt wird gewarnt, dass der DA (Datenbereitstellung) mit der

[317] Art 2 Z 12 DA; ErwGr 18 DA.

[318] In der Praxis werden wahrscheinlich Schwierigkeiten in der Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten, die durch IoT-Geräte verarbeitet werden, entstehen (zB mittels Sensoren erhobenes Ton-, Bild- oder audiovisuelles Material). Um Verstöße gegen die DSGVO zu vermeiden, wird der Dateninhaber daher im Zweifel solche Daten als personenbezogen einstufen müssen; vgl *Heinzke*, Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201 (201).

[319] Art 2 Z 14 DA.

[320] *Schwamberger*, Der Data Act, ecolex 2024/210, 367 (367).

[321] *Knapp/Kobler/Richter*, Data Cooperatives - Collective Action as an Opportunity for the European Data Economy and a European Data Private Law, InTeR 2023, 7 (7).

[322] *Gutjahr/Spiecker/Wilmer*, Systemische Privatheit für große, reale Datenverarbeitungssysteme, KuR 2024, 181 (181).

[323] *Humer*, Datenzugang nach dem Data Act und dem Digital Markets Act – Game-Changer für Start-ups? ZIIR 2024, 16 (17).

[324] *Heinzke/Herbers/Kraus*, Datenzugangsansprüche nach dem Data Act, BB 2024, 649 (649).

[325] *Podszun*, Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, in *Friedl/Burgi* (Hrsg), Wirtschaft und Recht für Mittelstand und Handwerk 8 (2023) 46.

DSGVO (Datenschutz) im Konflikt steht.[326] Es wäre angebracht, angesichts der zunehmend komplexen Wechselwirkungen zwischen den einzelnen EU-Rechtsakten im Bereich des Datenschutz- und Digitalrechts konsistente Formulierungen mit klaren Empfehlungen und Richtlinien zum bis dato ungeklärten Verhältnis[327] der Regelungen zueinander zu etablieren.[328]

Wie der DSA und DMA verbietet auch der DA den Einsatz von Dark Patterns (ErwGr 38 DA), dh „*Gestaltungstechniken, die dazu dienen, Verbraucher zu Entscheidungen, die negative Folgen für sie haben, zu verleiten oder sie zu täuschen*", wobei abermals „*übliche und rechtmäßige Geschäftspraktiken [...] an sich nicht als Dark Patterns angesehen werden*" sollten.[329] Art 6 Abs 2 lit a DA normiert das diesbezügliche Verbot.[330] Insgesamt wäre eine Klarstellung im Interesse der Rechtssicherheit wünschenswert, die feststellt, dass sich das Verbot auch auf die Zustimmung des Dateninhabers zur Weitergabe von Daten an Dritte erstreckt. Im Übrigen lässt der DA die Bestimmungen der UGP-RL unberührt (ErwGr 9 DA, Art 1 Abs 9 DA).

2.6 Deepfakes

Unter „*Deepfakes*" versteht man (durch KI) „*manipulierte Bild-, Audio- oder Videoinhalte, die wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise echt oder wahr erscheinen würden*" (vgl ErwGr 134 KI-VO). Zudem können manipulierte Texte als Deepfakes klassifiziert werden, welche gleichfalls eine signifikante Gefahr für Persönlichkeitsrechte[331] und die öffentliche Meinungsbildung darstellen.[332] Die Fülle an Informationen erschwert es immer häufiger, vertrauenswürdige Quellen von nicht vertrauenswürdigen zu unterscheiden, was zur Verbreitung von sog „*Fake News*" führt.[333]

[326] *Wiedemann/Conrad/Salemi*, Bereitstellung von Daten nach dem Data Act – offene Fragen und verbleibende Probleme, KuR 2024, 157 (157).
[327] *Mendelsohn/Richter* in *Steinrötter* (Hrsg) Europäische Plattformregulierung (2023) § 20 Rz 29.
[328] *Steinrötter*, Verhältnis von Data Act und DS-GVO, GRUR 2023, 216 (225 f).
[329] Im Gegensatz zu den ErwGr 29 KI-VO und 67 DSA fehlt hier jedoch die explizite Erwähnung von „*Werbung*".
[330] *Hofmeister/Giupponi*, The Regulation of the Data Economy, ZfRV 2023/103, 243 (243).
[331] *Linardatos*, Auf dem Weg zu einer europäischen KI-Verordnung, GPR 2022, 58 (68 f).
[332] *Kumkar/Rapp*, Deepfakes, ZfDR 2022, 199 (199 f).
[333] *Hartmann*, Der persönlichkeitsrechtliche Schutz vor Deepfakes, KuR 2020, 350 (350).

Die (potenziellen) Anwendungsfelder[334] von derartigen Methoden sind scheinbar grenzenlos: Relativ harmlos – da grds durch die Meinungs-, Kunst- und Pressefreiheit gedeckt – dürfte der Einsatz von Deepfakes für offensichtlich unterhaltsame, parodistische Zwecke sein, wie zB die Verwendung von Gesichtsfiltern oder das Erzeugen von lustigen Memes und Videos für soziale Medien.[335] Bedrohlich sind andererseits Szenarien, in welchen KI-Systeme in die Privatsphäre von Personen eingreifen,[336] indem sie Gesichter oder Stimmen verzerren ohne die (datenschutzrechtliche) Zustimmung der betroffenen Personen einzuholen.[337] Personen könnten bloßgestellt oder öffentlich gedemütigt und diskreditiert werden. Eine Person könnte fälschlicherweise Aussagen zugeschrieben bekommen oder Handlungen untergeschoben werden, die sie nie getätigt hat. Diesfalls tangieren Deepfakes auch das Strafrecht, weil va Beweismittel gefälscht oder verfälscht werden könnten.[338] Weiters könnten Cyberkriminelle[339] in Versuchung geraten, ganze Identitäten zu stehlen, (personenbezogene) Daten zu manipulieren und sich dadurch leichter Zugang zu sensiblen Informationen und finanziellen Ressourcen von Betroffenen zu verschaffen.[340] Im Gesellschaftsrecht kann es genauso zu Auswirkungen kommen.[341]

Ebenso könnten Deepfake-Techniken in der Werbung vielfältig genutzt werden: Unternehmen könnten sie bspw nutzen, um Prominente oder bekannte Persönlichkeiten als Sprecher in ihren Werbekampagnen zu präsentieren, was dazu beiträgt, das Interesse der Zielgruppe zu wecken und die Glaubwürdigkeit der Marke zu steigern. Denkbar ist auch eine Hyperpersonalisierung von Werbung.[342] Außerdem könnten Deepfakes verwendet werden, um Produkte oder Marken unauffällig in Filme, Videos oder andere Inhalte zu integrieren ohne dabei aufdringlich zu wirken. In Kombination mit Nudging oder Dark Patterns könnte eine subtile und effektive Methode geschaffen werden, um eigene Produkte zu bewerben und den Kauf anzuregen oder in missbräuchlicher Weise dazu zu verleiten. Zusammengefasst könnten solche

334 *Thiel*, „Deepfakes" – Sehen heißt glauben? ZRP 2021, 202 (202 f).
335 *Lantwin*, Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz? MMR 2019, 574 (574 f).
336 *Lennartz*, „Digitale Puppenspieler" – die Nachbildung von Körper und Stimme durch KI, NJW 2023, 3543 (Rz 1 ff).
337 *Grasser*, Herausforderungen einer vertrauenswürdigen Künstlichen Intelligenz, EALR 2020, 14 (17).
338 *Haag* in *Hoeren/Sieber/Holznagel* (Hrsg), Handbuch Multimedia-Recht[60.EL] (2023) Teil 29.5 Rz 28 ff.
339 *Drolz*, Mögliche Konsequenzen sowie Prävention eines Cyber-Vorfalls, GRC aktuell 2023, 49 (51).
340 *Lamprecht*, Hektik in der Cyberwelt, CFO aktuell 2023, 111 (113).
341 *Kommenda/Schwab*, Was tun, wenn sich künstliche Intelligenz unter die Gesellschafter mischt? AR aktuell 2023, 99 (101 f).
342 *Gräfe*, Webtracking und Microtargeting als Gefahr für Demokratie und Medien, DSRITB 2018, 27 (31).

Vorgehensweisen menschliches Verhalten erheblich beeinflussen und zu großen Schäden führen, insb finanzielle Nachteile verursachen.

Obwohl Deepfakes dank früherer Tools wie Photoshop schon lange möglich waren, sind die Barrieren für ihre Erstellung dank KI-Modellen deutlich gesunken.[343] Es wird augenscheinlich, dass in Zukunft die Bedeutung von Datensicherheit, der Förderung von Datenschutzbewusstsein und -bildung sowie der Entwicklung von (algorithmischen) Systemen zur frühzeitigen Erkennung und Verhinderung von Deepfakes enorm zunehmen wird. Andernfalls besteht mE das Risiko, dass man dem rasanten Fortschritt der Technologien konstant hinterherhinkt. Trotz allem scheinen die wahrgenommenen Vorteile von KI-Anwendungen bisher die (datenschutzrechtlichen) Bedenken zu überdecken. Dennoch sollten Werbetreibende stets beachten, dass mit zunehmender Intelligenz und Integration von KI-Anwendungen auch die Sorgen der angesprochenen Kunden bzgl Datenschutz, Sicherheit und Dateneigentum steigen.[344] Es wird daher voraussichtlich erforderlich sein, bestimmte Formen des Missbrauchs, tlw auch Deepfakes,[345] gesetzlich zu verbieten bzw unter Strafe zu stellen, denn „*die Frage ist nicht, ob wir KI wollen, sondern wie wir sie nicht wollen.*“[346] Immerhin wurden alle Vermittlungsdienstanbieter gem dem DSA verpflichtet, rechtswidrige („*illegale*“) Online-Inhalte zu identifizieren und zu entfernen.[347]

2.7 Profiling

2.7.1 Verbot ausschließlich automatisierter Entscheidungen im Einzelfall

Jede natürliche Person, deren personenbezogene Daten verarbeitet werden, hat auf der einen Seite das subjektive Recht, keiner „*ausschließlich auf einer automatisierten Verarbeitung –*

[343] *Werum*, Unbegrenzte Möglichkeiten – Deepfakes im Marketing, abrufbar unter <https://aric-hamburg.de/allgemein/deepfakes-werbung-marketing/?trk=article-ssr-frontend-pulse_little-text-block> (26.4.2024).
[344] *Pieper* in *Lucas/Schuster* (Hrsg), Innovatives und digitales Marketing in der Praxis (2023) 230.
[345] *Thurner*, Bildmanipulation und Persönlichkeitsschutz in Zeiten von „Deepfakes", MR 2019, 155 (161 f).
[346] *Grünzweig*, Welche Gesetze braucht künstliche Intelligenz? Die Presse - Recht 2023/359.
[347] *Bayer*, AI and disinformation, LTZ 2022, 81 (81).

einschließlich Profiling[348] – beruhenden Entscheidung[349] unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" (Art 22 Abs 1 DSGVO). Auf der anderen Seite statuiert Art 22 DSGVO ein allgemeines Verbot von derartigen nachteiligen Entscheidungen, das von den Verantwortlichen unter allen Umständen beachtet werden muss, selbst wenn die betroffene Person ihr korrespondierendes Recht nicht individuell geltend macht.[350]

Es ist wichtig zu betonen, dass sich Profiling auf jede Art der automatisierten Verarbeitung bezieht und nicht nur auf solche, die „*ausschließlich*" automatisiert sind. Da Profiling an sich nicht durch Art 22 DSGVO reguliert[351] bzw generell verboten[352] wird, kann es – wie bei jeder Datenverarbeitung – zulässig sein, wenn eine geeignete Rechtsgrundlage iSd DSGVO vorhanden ist und die Grundsätze einer Datenverarbeitung eingehalten wurden (ErwGr 72 DSGVO).[353] Eine unzulässige, ausschließlich automatisierte Entscheidung kann somit auch auf rechtmäßigem Profiling basieren.[354] Der Grundgedanke hinter Art 22 DSGVO besteht darin, sicherzustellen, dass eine Person nicht lediglich zum Objekt automatisierter Entscheidungen wird, wie sie etwa in einem vollständig algorithmusbasierten Datenverarbeitungsprozess vorkommen könnten.[355] Entscheidungen, welche die Bewertung einer Person inkludieren, dürfen nicht nur Maschinen überlassen werden.[356] Stattdessen sollte die menschliche Beurteilung ein integraler Bestandteil des Entscheidungsprozesses sein.[357]

---

[348] Das ist die in jeglicher Form automatisierte Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person, insb zur Analyse oder Prognose von Aspekten bzgl Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person (Art 4 Z 4 iVm ErwGr 71 Satz 2 DSGVO); vgl auch ErwGr 30 DSGVO: Online-Kennungen zur Profilerstellung und Identifizierung.

[349] Dabei geht es um die Bewertung von persönlichen Aspekten des Betroffenen ohne jegliches menschliche Eingreifen, wie zB die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren (ErwGr 71 Satz 1 DSGVO).

[350] *Helfrich* in *Sydow/Marsch* (Hrsg) DS-GVO/BDSG[3] (2022) Art 22 DSGVO Rz 40.

[351] Vgl aber das Profilingverbot im DA (Art 6 Abs 1 lit b DA iVm ErwGr 39 DA) und die bereits angesprochenen profilingbasierten Werbeverbote des DSA (Art 26 Abs 3 DSA und Art 28 Abs 2 DSA).

[352] Gegen die Verarbeitung für Zwecke der Direktwerbung und das damit verbundene Profiling ist jedoch ein jederzeitiger Widerspruch ohne Angabe von Gründen möglich (Art 21 DSGVO); vgl *Schmidl/Gerhalter*, Leitfaden zur Verordnung (EU) 2016/679 (Stand September 2022), 40, abrufbar unter <https://www.dsb.gv.at/download-links/ dokumente.html> (26.4.2024).

[353] *Frank-Woda/Steiner*, Datenschutz in der Unternehmenspraxis (2022) 56 ff.

[354] *Feiler/Forgó*, EU-DSGVO und DSG[2] (2022) Art 22 Rz 2, 5.

[355] *Martini* in *Paal/Pauly* (Hrsg), DS-GVO/BDSG[3] (2021) Art 22 Rz 1.

[356] *Knyrim* in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020) Kap 12 Rz 12.44.

[357] *Hladjk* in *Ehmann/Selmayr* (Hrsg), Datenschutz-Grundverordnung[2] (2018) Art 22 Rz 4.

Schon vor Verabschiedung der KI-VO wurde eigens darauf hingewiesen, dass KI und maschinelles Lernen leichter Profile erstellen können und (rein) automatisierte Entscheidungen getroffen werden, die die Rechte und Freiheiten des Einzelnen – auch in der Marketing- und Werbebranche – erheblich beeinträchtigen können,[358] wenngleich *„rechtlich nachteilige Entscheidungen über Menschen nur Menschen treffen [sollen]*."[359] Art 22 DSGVO beschränkt demgemäß auch die Entscheidungsfindung unter Verwendung von KI.[360] Aufgrund des technologischen Fortschritts und der Möglichkeiten neuer Big Data-Technologien ist für diese Art der eingriffsintensiven Datenverarbeitung ausdrücklich eine DSFA vorgesehen (Art 35 Abs 3 lit a DSGVO iVm ErwGr 91 Satz 2 DSGVO).[361]

Das Problem personalisierter Werbung im Kontext von Art 22 DSGVO liegt darin, dass die Schwelle der Erheblichkeit überschritten werden muss.[362] Einige Meinungen in der Literatur behaupten, dass automatisierte Entscheidungen über die Anzeige von werbebasiertem Profiling für den Betroffenen keine rechtlichen Auswirkungen haben und ihn nicht in ähnlicher Weise erheblich beeinträchtigen.[363] Auch das BVwG[364] folgt dieser These. Dementsprechend hätten grds auch personalisierte Preisangebote an sich keine rechtlichen Konsequenzen, da sie den Betroffenen noch nicht verpflichten.[365] Dem kann jedoch zu Recht entgegengehalten

---

[358] Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, 5, abrufbar unter <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_de> (26.4.2024).

[359] *Forgó*, „In technology, whatever can be done, will be done?" – Gibt es (datenschutz-)rechtliche Grenzen des Einsatzes von KI und, wenn ja, wo verlaufen diese? in *Reindl-Krauskopf/Grafl* (Hrsg), Künstliche Intelligenz – Fluch oder Segen (2020) 92.

[360] *Paal* in *Kaulartz/Braegelmann* (Hrsg), Rechtshandbuch Artificial Intelligence und Machine Learning (2020) Kap 8.7 Rz 9.

[361] Erläuterungen zur DSFA-V, § 2 Abs 2 Z 2, 2 f, abrufbar unter <https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html> (27.4.2024).

[362] Werbung für einen Mainstream-Modehändler, die sich auf ein einfaches demografisches Profil stützt, wie zB „*Frauen im Alter von 25 bis 35 Jahren im Raum Brüssel, die wahrscheinlich Interesse an Mode und bestimmten Bekleidungsartikeln haben*", wird Personen nicht in ähnlicher Weise erheblich beeinträchtigen; vgl Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, 24.

[363] *Engel/Napieralski* in *Forgó* (Hrsg), Grundriss Datenschutzrecht (2019) 89; *Von Lewinski* in *Wolff/Brink/von Ungern-Sternberg* (Hrsg), BeckOK Datenschutzrecht[47.EL] (2024) Art 22 Rz 34; krit *Martini* in *Paal/Pauly* (Hrsg), DS-GVO/BDSG[3] (2021) Art 22 Rz 27b.

[364] BVwG 2.9.2022, W214 2230686-1: Die Zuordnung von Marketing-Klassifikationen ist keine automatisierte Einzelentscheidung iSd Art 22 DSGVO.

[365] *Hofmann/Freiling*, Personalisierte Preise und das Datenschutzrecht, ZD 2020, 331 (332); krit *Linderkamp*, Der digitale Preis – eine automatisierte Einzelfallentscheidung? ZD 2020, 506 (508): Wenn jemand zB eine Flasche Wasser kaufen möchte und die Software eine Dehydrierung erkennt, könnten personalisierte Preise erhebliche Auswirkungen haben. Dies trifft jedoch nur zu, wenn der Unterschied zum Marktpreis besonders groß ist. Der Preisunterschied sollte reflektieren, dass der Vertrag unter normalen Umständen nicht zustande

werden, dass besonders aggressive Werbepraktiken, die unter die UGP-RL bzw das UWG fallen, die finanziellen Interessen einer Person durchaus beeinflussen können.[366] Bspw könnte sie dazu verleitet werden, teure Produkte zu kaufen, unerschwingliche Versicherungsverträge oder Online-Wetten[367] abzuschließen. Daher können solche rein automatisierten Entscheidungen ähnlich nachteilig sein wie die automatische Ablehnung einer Kreditanfrage.[368]

Nach Ansicht der Art-29-Datenschutzgruppe[369] sind va die folgenden Kriterien ausschlaggebend für die Annahme einer erheblichen Beeinträchtigung: (a) der invasive Charakter des Profiling-Prozesses, insb wenn Personen über verschiedene Websites, Geräte oder Dienste verfolgt werden, (b) die Erwartungen und Präferenzen der betroffenen Personen, (c) die Art und Weise, wie die Werbung präsentiert wird, und (d) die Ausnutzung von Schwachstellen bei den betroffenen Personen, an die sich die Anzeige richtet.

2.7.2 Durchbrechungen

Ausnahmen[370] vom Verbot gem Art 22 Abs 1 DSGVO bestehen nur, wenn die automatisierte Entscheidung im Einzelfall (i) für die Erfüllung eines Vertrags mit der betroffenen Person notwendig ist,[371] (ii) auf ihrer ausdrücklichen Einwilligung beruht, oder (iii) Rechtsvorschriften der EU oder ihrer MS[372] Profiling für zulässig erklären, sofern sie angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten (Art 22 Abs 2 DSGVO).

gekommen wäre. In diesem Fall wäre ein moralisches Gegengewicht erforderlich, das Menschen im Gegensatz zu Algorithmen setzen können, ua in Form einer Preisverhandlung.

366 *Feiler/Forgó*, EU-DSGVO und DSG[2] (2022) Art 22 Rz 7.

367 EDSA 13.4.2021, Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien[v2.0], Rz 88, abrufbar unter <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_de> (9.5.2024).

368 Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, 21 f.

369 Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, 24.

370 *Haidinger* in *Knyrim* (Hrsg), DatKomm Art 22 Rz 28 ff (Stand 1.12.2022, rdb.at).

371 *Spindler/Horváth* in *Spindler/Schuster* (Hrsg), Recht der elektronischen Medien[4] (2019) Art 22 Rz 10: Zu denken sei etwa an Bonitätsprüfungen für Darlehensverträge oder an Smart Meter, bei denen ein Unternehmen mit Energieverbraucheranalysen im Rahmen eines Vertragsverhältnisses beauftragt wurde.

372 *Taeger* in *Taeger/Gabel* (Hrsg), DSGVO/BDSG/TTDSG[4] (2022) Art 22 Rz 55.

Doch selbst dann dürfen solche automatisierten Entscheidungen grds nicht auf der Verarbeitung sensibler Daten beruhen.[373] Es sei denn, (i) die betroffene Person hat abermals eingewilligt, oder (ii) die Verarbeitung ist aus Gründen eines erheblichen öffentlichen Interesses erforderlich (Art 22 Abs 4 DSGVO).[374] Vorausgesetzt wird, dass sowohl eine unionsrechtliche oder mitgliedstaatliche Rechtsgrundlage existiert, die in einem angemessenen Verhältnis zum verfolgten Ziel steht und den Wesensgehalt des Rechts auf Datenschutz wahrt, als auch angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen vorgesehen sind.

In Bezug auf Kinder bleibt es jedoch beim Verbot gem Art 22 Abs 1 DSGVO (ErwGr 71 Satz 5 DSGVO),[375] solange eine Verarbeitung nicht ausnahmsweise zum Schutz ihres Wohlergehens erforderlich ist.[376] Kinder bedürfen eines speziellen Schutzes hinsichtlich ihrer personenbezogenen Daten, da sie sich der Risiken, Konsequenzen und ihrer Rechte iZm der Datenverarbeitung (noch) weniger bewusst sind. Dieser besondere Schutz sollte sich ua auf die Verwendung ihrer Daten für Werbung oder die Erstellung von Nutzerprofilen sowie auf die Erhebung ihrer Daten bei der Nutzung von Diensten erstrecken, die speziell für Kinder angeboten werden (ErwGr 38 DSGVO).

In jedem Fall sollte eine Verarbeitung mit angemessenen Garantien verbunden sein (Art 22 Abs 3 DSGVO),[377] einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen (Intervention) einer Person,[378] auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf eine (außergerichtliche) Anfechtung der Entscheidung (ErwGr 71 Satz 4 DSGVO). Dies soll eine faire und transparente Verarbeitung (ErwGr 60 DSGVO) gegenüber dem Betroffenen gewährleisten (ErwGr 71 Satz 6 DSGVO),[379] um va

[373] VwGH 14.12.2021, Ro 2021/04/0007, Rz 45; OGH 15.4.2021, 6 Ob 35/21x: Die Notwendigkeit dieser Regelung ergibt sich aus dem hohen Schadens- und Diskriminierungspotenzial, das von automatisierten Entscheidungen ausgeht, welchen besondere Kategorien personenbezogener Daten zugrunde liegen.

[374] *Von Lewinski* in *Wolff/Brink/von Ungern-Sternberg* (Hrsg), BeckOK Datenschutzrecht[47.EL] (2024) Art 22 Rz 60.

[375] *Jahnel* in *Jahnel* (Hrsg), DSGVO Art 22 Rz 33 (Stand 1.12.2020, rdb.at).

[376] Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, 31.

[377] *Steinrötter* in *Borges/Hilber* (Hrsg), BeckOK IT-Recht[13.EL] (2023) Art 22 Rz 15.

[378] Dh, dass auf Seiten des datenschutzrechtlich Verantwortlichen mind ein Mensch vorhanden sein muss, der befugt ist, in die automatisierte Entscheidung einzugreifen, um diese gegebenenfalls zu korrigieren.

[379] Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, 27: Mit verstärktem Einsatz und wachsender Komplexität des maschinellen

Diskriminierungen vorzubeugen.[380] Transparenz gilt „*insb für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet*" (ErwGr 58 Satz 3 DSGVO). Das bedeutet, dass der Betroffene einerseits über die automatisierte Entscheidungsfindung – das „*Ob*" und „*Wie*"[381] – informiert werden muss (Art 13 Abs 2 lit f DSGVO bzw Art 14 Abs 2 lit g DSGVO)[382] und er andererseits ein subjektives Recht hat, zu erfahren, warum diese im konkreten Fall zu einer für ihn nachteiligen Situation geführt hat, damit er evtl selbst geeignete Maßnahmen ergreifen kann, um dies zu berichtigen.[383] Das Auskunftsrecht (Art 15 Abs 1 lit h DSGVO iVm ErwGr 63 DSGVO) bietet dem Betroffenen insofern eine Erleichterungs-möglichkeit, indem er Informationen über die angewandte Logik sowie die Tragweite und die angestrebten Auswirkungen einer solchen Verarbeitung erhalten kann.[384]

Unter der „*involvierten Logik*" versteht man mittlerweile auch aussagekräftige Erklärungen hinsichtlich der verwendeten Algorithmen von Scoring-Verfahren[385] sowie der mithilfe von KI bzw neuronalen Netzen gefundenen Ergebnisse.[386] Besonders bei technisch komplexen Systemen kann es so gesehen eine Herausforderung sein, eine für den betroffenen Laien verständliche Beschreibung bereitzustellen. Dennoch darf die Offenlegung nicht allein aufgrund der Komplexität verweigert werden.[387] Im Gegenteil, je komplexer das System ist, desto höher sind die Anforderungen an die Informationsbereitstellung. Nur auf diese Weise kann der Betroffene nachvollziehen, ob irrelevante Daten oder sachfremde Erwägungen in die automatisierte Entscheidung einfließen und somit seine Rechte effektiv geltend machen.[388] Die genaue

Lernens wird es zusehends herausfordernder, die Funktionsweise automatisierter Entscheidungsfindung oder des Profiling zu verstehen.

380 *Schulz* in *Gola/Heckmann* (Hrsg), DS-GVO/BDSG[3] (2022) Art 22 Rz 2: Die DSGVO schweigt allerdings über die eigentlich dringend zu regelnden (manipulativen) Gefahren für die Grundrechte und Freiheiten des Einzelnen, die in den Algorithmen selbst liegen können, wie bspw algorithmische Verzerrungen („*Algorithmic Bias*").

381 *Martini/Nink*, Wenn Maschinen entscheiden …, NVwZ 2017, 681 (682).

382 *Pollirer/Knyrim* in *Knyrim* (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020) Kap 20 Rz 20.36.

383 *Buchner* in *Kühling/Buchner* (Hrsg) DS-GVO/BDSG[4] (2024) Art 22 Rz 32 ff.

384 *Haidinger* in *Knyrim* (Hrsg), DatKomm Art 15 Rz 44 ff (Stand 1.12.2021, rdb.at).

385 *Roßnagel/Nebel/Richter*, Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455 (458).

386 *Dix* in *Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 22 Rz 25 f.

387 *Scholz* in *Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 22 Rz 58.

388 *Jungkind/Koch* in *Chibanguza/Kuß/Steege* (Hrsg), Künstliche Intelligenz (2022) § 4 D Rz 55.

Bandbreite des Informationsrechts und ob KI-Entwickler (die Verantwortlichen) in Kauf nehmen müssen, Geschäftsgeheimnisse preiszugeben,[389] bleibt umstritten[390] und kann in diesem Rahmen nicht ausführlich behandelt werden.

2.7.3 Scoring

Als Unterfall des Profiling[391] ermöglicht „*Scoring*" die Ermittlung sog „*Score-Werte*",[392] welche auf der Grundlage mathematisch-statistischer Berechnungsverfahren die persönlichen Aspekte in Bezug auf die wirtschaftliche Lage – dh, die Kreditwürdigkeit bzw Bonität – einer natürlichen Person analysieren und vorhersagen.[393] Je geringer der Score-Wert einer Person ist, desto höher ist die Wahrscheinlichkeit ihrer Zahlungsunfähigkeit.

In den Mittelpunkt der datenschutzrechtlichen Auseinandersetzung rückte das Scoring jüngst durch die fragwürdige Praxis der SCHUFA,[394] die eine vollautomatisierte Berechnung der vermeintlichen Kreditwürdigkeit anhand undurchsichtiger Algorithmen vornahm.[395] Dieser Vorgehensweise hat nun der EuGH[396] einen Riegel vorgeschoben, in dem er feststellte, dass „*eine automatisierte Entscheidung im Einzelfall [...] vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich[397] abhängt, ob ein Dritter, dem*

[389] Gem ErwGr 63 Satz 5 DSGVO darf das Auskunftsrecht die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insb das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass dem Betroffenen jegliche Auskunft verweigert wird (ErwGr 63 Satz 6 DSGVO).

[390] *Dürager* in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2019 (2019) 390 f; *Helfrich* in *Sydow/Marsch* (Hrsg), DS-GVO/BDSG[3] (2022) Art 22 Rz 79; *Arning* in *Moos/Schefzig/Arning* (Hrsg), Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6 Rz 65 ff (Stand 1.4.2021, rdb.at); *Conrad* in *Auer-Reinsdorff/Conrad* (Hrsg), Handbuch IT- und Datenschutzrecht[3] (2019) § 34 Rz 775.

[391] *Martini* in *Paal/Pauly* (Hrsg), DS-GVO/BDSG[3] (2021) Art 22 Rz 24.

[392] *Krämer*, Die Rechtmäßigkeit der Nutzung von Scorewerten, NJW 2020, 497 (497 ff).

[393] *Buchner* in *Kühling/Buchner* (Hrsg) DS-GVO/BDSG[4] (2024) Art 22 Rz 22.

[394] Die SCHUFA Holding AG ist eine dt Wirtschaftsauskunftei, welche ihre Kunden mit Informationen zur Bonität Dritter (Verbraucher und Unternehmen) versorgt.

[395] Noyb 7.12.2023, EuGH weist Kreditauskunftei SCHUFA in die Schranken, abrufbar unter <https://noyb.eu/de/cjeu-landmark-rulings-credit-ranking-and-review-dpas> (28.4.2024).

[396] EuGH 7.12.2023, C-634/21 (*SCHUFA Holding AG*) Rz 73, 75.

[397] *Blasek*, Die Rolle von Scorewerten bei automatisierten Entscheidungen, ZD 2024, 258 (259): Das vom EuGH eingeführte und nicht weiter definierte Maßgeblichkeitskriterium wird je nach der jeweiligen Branche im konkreten Fall betrachtet werden müssen; vgl auch DSB 20.12.2023, D036.500 (2023-0.891.733): Kreditauskunfteien können sich nicht mehr pauschal auf ihr berechtigtes Interesse stützen, sondern nur auf eine Ausnahmebestimmung im Einzelfall gem Art 22 Abs 2 DSGVO.

dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet."[398] Selbst eine nachgelagerte menschliche Entscheidung auf Basis dieses automatisch generierten Score-Werts kann das Merkmal einer reinen Automatisierung nicht aufheben, sofern die menschliche Entscheidung „*rein formalen Charakter*" hat.[399] Schließlich würden Kunden (ua Banken)[400] der SCHUFA den Score-Wert ihrer eigenen Entscheidung – der konkreten Gewährung oder Nichtgewährung eines Kredits – idR ungeprüft zugrunde legen.[401] Bei KI-Systemen[402] ist es daher ebenso entscheidend, dass der menschliche Entscheidungsträger die Autorität zur letzten Entscheidung hat und den Vorschlag einer KI nicht unüberlegt akzeptiert,[403] denn „*mit dieser EuGH-Entscheidung wurde der Anwendungsbereich des Art 22 DSGVO und damit jener der datenschutzrechtlichen Regulierung künstlicher Intelligenz erheblich erweitert*."[404]

In Österreich wurde der sog „*AMS-Algorithmus*"[405] eingesetzt, um Arbeitssuchende in verschiedene Gruppen zu kategorisieren, abhängig von ihren jeweiligen Arbeitsmarktchancen.[406] Eine höhere errechnete Wahrscheinlichkeit für eine erfolgreiche Arbeitsvermittlung führte zu einer intensiveren Betreuung durch Mitarbeiter des AMS. Die DSB[407] war der Meinung, dass die menschliche Entscheidung durch diese Berechnungen erheblich beeinflusst wurde, selbst wenn die Ergebnisse nicht unhinterfragt übernommen wurden.[408] Das BVwG[409] hingegen vertrat einen anderen Standpunkt und argumentierte, dass die Mitarbeiter den AMS-Algorithmus lediglich als Hilfsmittel verwendeten, sodass keine automatisierte Entscheidung iSv Art 22 DSGVO vorlag.[410] Letztendlich kam der VwGH[411] zum Schluss, dass zwar ein (erhebliches)

[398] *Salomon/Trieb*, Ermittlung eines Score-Werts kann das Verbot der automatisierten Entscheidung (Art 22 DSGVO) verletzen, ZFR 2024/50, 119 (119 ff).
[399] GA *Pikamäe*, SA 16.3.2023, C-634/21 (*SCHUFA Holding AG*) Rz 47.
[400] *Blasek*, Auskunfteiwesen und Kredit-Scoring in unruhigem Fahrwasser, ZD 2022, 433 (434).
[401] *Hessel/Dillschneider*, Datenschutzrechtliche Herausforderungen beim Einsatz von Künstlicher Intelligenz, RDi 2023, 458 (463 f).
[402] *Kern*, Automatisierte Entscheidungsfindung nach Art 22 DSGVO bei bloß entscheidungsunterstützenden Systemen wie zB Scoring, ecolex 2024/112, 191 (191).
[403] *Malorny*, Datenschutz als Grenze KI-basierter Auswahlentscheidungen im Arbeitsrecht, RdA 2022, 170 (176 f).
[404] *Feiler/Brandauer*, Strenge Regulierung künstlicher Intelligenz bereits in Geltung, AnwBl 2024/122, 258 (258).
[405] „*Arbeitsmarktchancen-Assistenzsystem*" („*AMAS*").
[406] *Bachberger-Strolz*, Profiling, Targeting, Algorithmen, künstliche Intelligenz – über die Irrwege einer Debatte in der Arbeitsmarktpolitik, WuG 2020, 329 (329 ff).
[407] DSB 16.8.2020, D123.1020 (2020–0-513.605).
[408] *Thiele*, DSB stattet AMS-Algorithmus mit Ablaufdatum aus, ZIIR 2020, 410 (417).
[409] BVwG 18.12.2020, W256 2235360-1.
[410] *Gerhartl*, Betrachtungen zum AMAS-Algorithmus, ZIIR 2021, 24 (27 f).
[411] VwGH 21.12.2023, Ro 2021/04/0010.

öffentliches Interesse an den Beratungsleistungen durch das AMS – *in concreto* in Form des Funktionierens des Arbeitsmarkts[412] – besteht, doch handelt es sich bei der Errechnung der Arbeitsmarktchancen durch das AMAS um Profiling. Der VwGH bezog sich dabei auf das *SCHUFA*-Urteil des EuGH, wonach das Ergebnis eines Profilings eine automatisierte Einzelfallentscheidung iSd Art 22 DSGVO darstellt, wenn das Handeln eines Dritten (hier: AMS-Mitarbeiter) maßgeblich durch den automatisch errechneten Wert beeinflusst wird. Das österreichische Höchstgericht hob die BVwG-Entscheidung aus diesem Grund auf. Im weiteren Verfahren wird das BVwG im Rahmen einer mündlichen Verhandlung die Rechtslage unter Berücksichtigung der dargestellten Rechtsprechung mit den Parteien erörtern.[413]

2.8 Fazit

KI nimmt im Marketing eine immer bedeutendere Rolle ein. Feststellen lassen sich deutliche Verbesserungen in Effizienz und Ergebnissen. Trotz dieser vielfältigen Vorteile sind mit dem Einsatz von KI in der Online-Werbung auch Herausforderungen und Risiken verbunden, insb in Bezug auf Datenschutz und Vertrauensfragen, die bereits vor dem KI-Einsatz sorgfältig geprüft werden müssen.

In der Praxis zeigt sich, dass viele, insb fragwürdige, Anwendungen KI-gesteuerter Marketingmaßnahmen in den USA entwickelt und eingesetzt werden. Dies liegt vermutlich daran, dass die Datenschutzbestimmungen dort weniger streng sind als in Europa. Darüber hinaus herrscht in den USA ein anderes gesellschaftliches Verständnis und eine positivere Einstellung gegenüber neuartigen Technologien. Eine kritische Auseinandersetzung mit den damit verbundenen Risiken bleibt oft aus. Die USA haben nämlich eine stark wettbewerbsorientierte Wirtschaft, die technologischen Fortschritt und Innovationen begünstigt. Amerikaner neigen daher dazu, neue Technologien schnell zu adaptieren und deren Vorteile zu schätzen, auch wenn dies mit gewissen Risiken für ihre Grundrechte verbunden ist. Hingegen herrschen in Europa oft mehr Vorsicht und Skepsis. Dies spiegelt sich auch in der öffentlichen Wahrnehmung wider: In den USA gibt es tendenziell positivere Berichterstattung über KI und deren

[412] Das AMS-Gesetz, BGBl Nr 313/1994 idF BGBl I Nr 174/2023, beschreibt den Zweck der Datenverarbeitung (Arbeitsvermittlung) hinreichend klar und bestimmt (vgl §§ 25, 29 AMS-Gesetz).

[413] *Kriwanek/Tuma*, Datenschutz: Arbeitsmarktchancen-Assistenzsystem (AMAS) (16.02.2024, LexisNexis Rechts news 35079 in lexis360.at).

Vorteile. Medien und Unternehmen betonen oft die praktischen Aspekte, was die öffentliche Meinung zugunsten dieser Technologie beeinflusst. In der EU und in den MS sind es hingegen va NGOs und die Zivilgesellschaft, die konsequent vor dem Einsatz von KI warnen.

Unternehmen könnten nun in Versuchung geraten, solche oftmals bedenklichen Werbepraktiken gleichfalls in Europa zu etablieren. In einem globalen Marktumfeld streben auch sie letztlich nach Effizienz und Wettbewerbsfähigkeit. Angesichts des aktuellen Hypes um KI befürchten viele Unternehmen, den Anschluss zu verlieren, wenn sie nicht ebenfalls solche Technologien einsetzen. Dabei geraten wichtige Aspekte wie Datenschutz – aber auch Verbraucherschutz – oft in den Hintergrund, obwohl in den letzten Jahren wiederholt schwere Verstöße gegen die DSGVO aufgetreten sind. Insgesamt besteht die Gefahr also darin, dass KI-gesteuerte Marketingpraktiken in Europa möglicherweise nicht immer im Einklang mit den strengen Datenschutzstandards der EU stehen.

Jedoch bleibt festzuhalten, dass der Einsatz von KI stets den Vorgaben der DSGVO entsprechen muss. Dies gilt auch nach der Einführung der KI-VO, wie im weiteren Kapitel dieser Arbeit näher erläutert wird.

3 KI-VO & Online-Werbung

Das vorhergehende Kapitel zeigt, dass viele datenschutzrechtliche Fragen und Herausforderungen iZm Online-Werbung und KI keineswegs Neuland sind. Sie waren und sind bereits intensiver Gegenstand juristischer Lehre und Rsp, lange bevor das EP die KI-VO billigte. Dieses Kapitel der Arbeit zielt nun darauf ab, festzustellen, ob und inwiefern es der KI-VO gelungen ist, die aufgezeigten Probleme einzudämmen.

3.1 Vorbemerkungen zur KI-VO

Der Übergang von der reinen KI-Beratung zur tatsächlichen KI-Entscheidung ist fließend und wird nicht immer erkannt, wodurch kommerziell motivierter Missbrauch und weitreichende Verbrauchermanipulation begünstigt werden.[414] Die kontinuierliche Weiterentwicklung von KI-Systemen nach ihrer Markteinführung, insb im Hinblick auf antrainierte oder sogar selbsterlernte Entscheidungsparameter, birgt erhebliche Risiken. Oft werden diese aber zugunsten von Effizienz, Komfort und einer stärkeren Normalisierung des Einsatzes von KI-Technologien ausgeblendet.[415] Es ist jedoch positiv anzumerken, dass die KI-VO grds innovationsoffen[416] – aber nicht technologieneutral[417] wie zB die DSGVO – konzipiert wurde. Sie versucht, zukünftige Entwicklungen zumindest angemessen zu berücksichtigen,[418] ohne dabei zukunftsweisendes Engagement zu behindern und dadurch unvermeidbare Wettbewerbsverluste[419] zu riskieren.[420] Es gibt andererseits auch berechtigte Kritik hinsichtlich des risikobasierten Ansatzes,[421] den die KI-VO verfolgt. Dieser erscheint nicht immer schlüssig und weist erhebliche Lücken

[414] *Hilgendorf* in *Fischer* (Hrsg), Beweis (2019) 229.

[415] *Gless/Janal* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 2 Rz 3.

[416] Vgl die Definition eines KI-Systems (Art 3 Z 1 KI-VO): Ein KI-System ist „*ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können*." Es brauche nämlich „*Flexibilität, um den raschen technologischen Entwicklungen [...] Rechnung zu tragen*" (ErwGr 12 KI-VO).

[417] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 151: Datenschutz ist auf verschiedene Technologien ausgerichtet („*technologieübergreifend*"), während die Regulierung von KI im Gegensatz dazu technologiebezogen („*technologiespezifisch*") ist.

[418] *Pohle*, Innovativ – und jetzt? CB 2021, 371 (372).

[419] Durch die Verbesserung von Vorhersagen, die Optimierung von Abläufen, Ressourcenallokation und die Personalisierung digitaler Lösungen – was meiner Meinung nach auch die Werbebranche betrifft – kann die Verwendung von KI Unternehmen bedeutende Wettbewerbsvorteile verschaffen (vgl ErwGr 4 KI-VO).

[420] *Ammann/Pohle*, KI-Verordnung – Was bisher geschah und jetzt zu tun ist, CB 2024, 137 (138).

[421] *J. Wendt/D. Wendt*, Einigung auf Rechtsrahmen für Künstliche Intelligenz in der EU: AI Act, ZfPC 2024, 86 (86).

auf,[422] wie zB im Hinblick auf die zuvor dargestellten Gefahren, die vom Marketingsektor ausgehen. Es ist bedauerlich, dass die KI-VO – wohl politischen Differenzen geschuldet – mit zahlreichen Ausnahmen und unklaren (Rechts-)Begriffen versehen wurde, wodurch sich für Anbieter,[423] Importeure,[424] Händler[425] und Betreiber[426] uU Compliance-Herausforderungen[427] ergeben könnten.[428] Darüber hinaus werden viele potenziell schädliche KI-Anwendungen nicht automatisch als Hochrisiko-KI eingestuft, geschweige denn als verbotene KI-Praktiken, obwohl eine solche Klassifizierung durchaus – iSd Rechtssicherheit – geboten wäre.[429] Dies verdeutlicht die dringende Notwendigkeit, die Regulierung von KI-gestützter oder sogar KI-autonomer Online-Werbung zu verschärfen,[430] wofür die EK ihre (Leitlinien-)Kompetenzen umfassend nutzen sollte.[431] Die nachstehenden Überlegungen sollen zeigen, warum dies mehr denn je angebracht ist, wenn man sich folgende Ziele der KI-VO verinnerlicht: die Einführung und Förderung einer auf den Menschen ausgerichteten, vertrauenswürdigen und ethisch vertretbaren KI („*human centric approach*", vgl ErwGr 6 und ErwGr 8 KI-VO)[432] sowie die Gewährleistung eines hohen Schutzniveaus in Bezug auf die in der GRC[433] verankerten Grundrechte vor schädlichen Auswirkungen von KI-Systemen in der Union (Art 1 Abs 1 KI-VO iVm ErwGr 1

[422] *Dix/Seyerlein-Klug*, EAID: Exportschlager AI Act – Setzt die EU einen weltweiten Standard für die KI-Regulierung? ZD-Aktuell 2024, 04506 (beck-online).

[423] Das ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder eine GPAI entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich (Art 3 Z 3 KI-VO); vgl Art 25 KI-VO iVm ErwGr 84 KI-VO zum Begriff des „*Scheinanbieters*".

[424] Das ist eine in der EU ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt (Art 3 Z 6 KI-VO: „*Einführer*").

[425] Das ist eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, außer es handelt sich dabei um den Anbieter oder Importeur (Art 3 Z 7 KI-VO).

[426] Das ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet (Art 3 Z 4 KI-VO). Wie die DSGVO (Art 2 Abs 2 lit c DSGVO) kennt die KI-VO eine „*Haushaltsausnahme*" bzgl KI-Systemen, die von natürlichen Personen für rein persönliche, nicht-berufliche Tätigkeiten verwendet werden (Art 2 Abs 10 KI-VO).

[427] Nicht zuletzt weil Verstöße gegen die in Art 5 KI-VO normierten Verbote mit Geldbußen von bis zu 35 Mio Euro oder bis zu 7 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden (Art 99 Abs 3 KI-VO).

[428] *Ashkar/Schröder*, Das Gesetz über künstliche Intelligenz der Europäischen Union (KI-Verordnung), BB 2024, 771 (771).

[429] *Hinderks*, Die Kennzeichnungspflicht von Deepfakes, ZUM 2022, 110 (117): Es wäre durchaus sinnvoll, die Einstufung von Deepfake-Technologien zumindest als Hochrisiko-KI-Systeme in Betracht zu ziehen.

[430] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 104 ff.

[431] Vgl insb Art 6 Abs 5-6, Art 7 Abs 1 (iVm Anhang III KI-VO), Art 11 Abs 3, Art 43 Abs 5, Art 47 Abs 5, Art 51 Abs 3, Art 52 Abs 4, Art 53 Abs 5-6 und Art 97 KI-VO.

[432] *Klaushofer*, Die menschenrechtliche Dimension Künstlicher Intelligenz, ZÖR 2019, 399 (411).

[433] Charta der Grundrechte der Europäischen Union, ABl 2016/C 202, 389.

ff KI-VO). Der tatsächliche Grundrechtsschutz wurde für Individuen allerdings – mE bewusst[434] – vernachlässigt. Es gibt zwar ein Beschwerderecht bei der Marktaufsichtsbehörde (Art 85 KI-VO) und ein gewisses Recht auf Erläuterung der Entscheidungsfindung einer Hochrisiko-KI im Einzelfall (Art 86 KI-VO iVm ErwGr 171 KI-VO), doch bieten sie gerade keinen „*traditionellen Grundrechtsschutz*".[435] Man möge umgehend meinen, dass die vom Europarat erarbeitete „*KI-Konvention*"[436] als zusätzliches Instrument auf europäischer Ebene dienen könnte, um die Menschenrechte in Bezug auf Datenschutz, Transparenz,[437] Verantwortlichkeit und den Schutz der Privatsphäre zu stärken. Diese wurde aber „*zahnlos*" ausgestaltet,[438] weil einige Formulierungen offensichtlich zu vage sind, wodurch die konkrete Umsetzung und Durchsetzung erschwert wird. Des Weiteren fehlen effektive Mechanismen zur Überwachung, sodass die Wirksamkeit der KI-Konvention insgesamt beeinträchtigt ist.[439]

3.2 Verbote verhaltensmanipulierender KI-Systeme

Bei der Analyse der KI-VO liegt zunächst der Fokus auf der Überprüfung potenzieller Überschneidungen der Inhalte von Kapitel 2 dieser Arbeit mit den Vorschriften über verbotene KI-Praktiken gem Art 5 KI-VO. Wichtig sind hierbei die Verbote, die auf Verhaltenslenkung abzielen, da sie im Marketingbereich besonders relevant sind.

---

[434] Denn im ErwGr 170 KI-VO steht explizit, dass „*im Unionsrecht und im nationalen Recht bereits wirksame Rechtsbehelfe für natürliche und juristische Personen vorgesehen [sind], deren Rechte und Freiheiten durch die Nutzung von KI-Systemen beeinträchtigt werden.*" Nichtsdestotrotz gesteht ErwGr 5 KI-VO ein, dass „*KI je nach den Umständen ihrer konkreten Anwendung und Nutzung sowie der technologischen Entwicklungsstufe Risiken mit sich bringen und [...] grundlegende Rechte schädigen [kann], die durch das Unionsrecht geschützt sind. Ein solcher Schaden kann materieller oder immaterieller Art sein, einschließlich physischer, psychischer, gesellschaftlicher oder wirtschaftlicher Schäden*."

[435] *Eisenberger* 18.4.2024, KI regulieren: Tun wir das Richtige? abrufbar unter <https://rudolphina.univie.ac.at/ki-regulieren-tun-wir-das-richtige> (30.4.2024).

[436] Ministerkomitee des Europarats 15.3.2024, CM(2024)52-prov1, abrufbar unter <https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411> (30.4.2024).

[437] „*Transparenz*" bedeutet, dass KI-Systeme so entwickelt und verwendet werden, dass sie angemessen nachvollziehbar und erklärbar sind, wobei den Menschen bewusst gemacht werden muss, dass sie mit einem KI-System kommunizieren oder interagieren, und dass die Betreiber ordnungsgemäß über die Fähigkeiten und Grenzen des KI-Systems informieren und die betroffenen Personen über ihre Rechte in Kenntnis setzen müssen (ErwGr 27 KI-VO). Die DSGVO versteht unter Transparenz, dass personenbezogene Daten ausschließlich in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden dürfen (Art 5 Abs 1 lit a DSGVO).

[438] *Sommer* 22.3.2024, Europaratskommission verabschiedet zahnlose KI-Konvention, abrufbar unter <https://www.digitale-gesellschaft.ch/2024/03/22/europaratskommission-verabschiedet-zahnlose-ki-konvention-wieviel-transparenz-vertraegt-geopolitik> (30.4.2024).

[439] Vgl auch die Kritik der Parlamentarischen Versammlung des Europarats 18.4.2024, Opinion 303 (2024), 2 f, abrufbar unter <https://pace.coe.int/en/files/33517> (30.4.2024).

3.2.1 Verhaltensmanipulation iSv Art 5 Abs 1 lit a KI-VO

Gänzlich verboten wird „*das Inverkehrbringen,*[440] *die Inbetriebnahme*[441] *oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird*."

Angesprochen wird hiermit das Selbstbestimmungsrecht – Autonomie, Entscheidungsfindung und freie Auswahl – der EU-Bürger als Fundament der europäischen Werteordnung,[442] um diese vor dem verpönten Einsatz von Dark Patterns und Nudging-Techniken („*manipulative oder täuschende Techniken")* zu schützen.[443] Manipulative, ausbeuterische und soziale Kontrollpraktiken sollen aufgrund ihres schädlichen und missbräuchlichen Charakters – auch im privaten Sektor[444] – verboten werden. Solche Praktiken stehen im Widerspruch zu den Werten der Union sowie den Grundrechten, inkl des Rechts auf Nichtdiskriminierung, Datenschutz und Privatsphäre sowie den Rechten der Kinder (ErwGr 28 KI-VO). Diese KI-Systeme nutzen geradezu subtile Beeinflussungsmethoden,[445] wie etwa Reize in Form von Tönen, Bildern oder Videos, welche für Menschen nicht erkennbar sind, da sie außerhalb ihres

[440] Das ist die erstmalige Bereitstellung eines KI-Systems oder einer GPAI auf dem Unionsmarkt (Art 3 Z 9 KI-VO). „*Bereitstellung auf dem Markt*" ist die (un-)entgeltliche Abgabe eines KI-Systems oder einer GPAI zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit (Art 3 Z 10 KI-VO).

[441] Das ist die Bereitstellung eines KI-Systems in der EU zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung (Art 3 Z 11 KI-VO).

[442] *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 2 f.

[443] Die Empfehlungssysteme von VLOPs sind darunter jedoch nicht zu subsumieren, weil sie bereits von anderen EU-Rechtsvorschriften – DSA und DMA – erfasst werden; vgl EK 12.12.2023, Künstliche Intelligenz – Fragen und Antworten, 4, abrufbar unter <https://ec.europa.eu/commission/presscorner/api/files/document/print/de/qanda_21_1683/QANDA_21_1683_DE.pdf> (2.5.2024).

[444] *Rostalski/Weiss*, Der KI-Verordnungsentwurf der Europäischen Kommission, ZfDR 2021, 329 (338).

[445] *Uuk* 18.1.2022, Future of Life Institute: Manipulation and the AI Act, 2, abrufbar unter <https://futureoflife.org/wp-content/uploads/2022/08/FLI-Manipulation_AI_Act.pdf> (5.5.2024): Es wäre besser gewesen, das Tatbestandsmerkmal „*unterschwellig*" gänzlich zu streichen.

Wahrnehmungsbereichs liegen. Doch selbst wenn sich Menschen dessen bewusst sind, können sie diesen Techniken nicht widerstehen oder sie kontrollieren (ErwGr 29 KI-VO). Zudem dürfte personalisierte Werbung an sich[446] unter den Begriff „*Beeinflussung*" fallen.[447]

Allerdings wird inzwischen[448] – und wie in der Einleitung (Kapitel 1) dieser Arbeit angedeutet – explizit festgehalten, dass übliche und rechtmäßige Praktiken, wie zB im Bereich der Werbung, nicht als schädlich-manipulativ betrachtet werden sollen (ErwGr 29 letzter Satz KI-VO). Problematisch ist, dass eine klare Definition fehlt, was als „*übliche*" und „*rechtmäßige*" Werbepraktiken betrachtet werden kann. Angesichts der Tatsachen, dass bereits jetzt viele Praktiken als unlauter gelten, da sie irreführend oder aggressiv sind, und dass der Einsatz von KI-Technologien die Möglichkeiten für Werbetreibende exponentiell erweitert, besteht die Gefahr, dass noch schädlichere – mithin „*unübliche*" – Praktiken entwickelt werden könnten, die dem Verbraucher- und Datenschutz abträglich sind. Weiters besteht die Ungewissheit, dass sich diese „*unüblichen*" Praktiken mit der Zeit zu „*üblichen*" entwickeln könnten, falls sie sich entsprechend in der Praxis etablieren sollten.

Gem ErwGr 29 KI-VO ergänzt Art 5 Abs 1 lit a KI-VO die UGP-RL.[449] Dennoch bleibt die KI-VO hinsichtlich der genauen Beziehung zwischen diesen beiden EU-Rechtsakten unklar, was einen weiteren Bedarf an Konkretisierung seitens der EK signalisiert. Interessant ist mE in diesem Zusammenhang, dass das Verbot gem Art 5 Abs 1 lit a KI-VO erst bei „*erheblicher*" Schadenszufügung durch KI-Systeme greifen soll, obwohl ErwGr 29 KI-VO vorsieht, dass „*unlautere Geschäftspraktiken*", durch die Verbraucher „*wirtschaftliche oder finanzielle Schäden*" erleiden, „*unter allen Umständen verboten*" sein sollen, und zwar „*unabhängig davon, ob sie durch KI-Systeme oder anderweitig umgesetzt*" werden. Somit sollten Unternehmen keine KI-Systeme – einschließlich grds unbedenklichen GPAI ohne systemisches Risiko (iSv „*anderweitig umgesetzt*")[450] – einsetzen dürfen, die Verbrauchern Schäden wirtschaftlicher oder finanzieller Art

[446] *Bastians* in *Steinrötter* (Hrsg) Europäische Plattformregulierung (2023) § 21 Rz 22: Behavioral Microtargeting könnte erfasst sein, bei welchem Einzelpersonen auf der Grundlage von personalisierten Nutzerprofilen, die Verhaltens- und Persönlichkeitsmerkmale umfassen, individuell angesprochen werden.

[447] *Bomhard/Merkle*, Europäische KI-Verordnung, RDi 2021, 276 (279).

[448] Im ursprünglichen Entwurf der KI-VO fehlte dieser Zusatz.

[449] Außerdem berührt die KI-VO verbraucherschutzrechtliche EU-Rechtsakte nicht (Art 2 Abs 9 KI-VO).

[450] Damit KI-Modelle zu KI-Systemen werden, ist grds die Hinzufügung weiterer Komponenten, zB einer Nutzerschnittstelle, erforderlich. KI-Modelle sind aber idR ohnehin in KI-Systeme integriert und Teil davon (ErwGr 97 KI-VO), sodass die hier getroffene Annahme eines weitreichenden Verbots auch für GPAI gelten könnte.

– ua durch den Einsatz von Dark Patterns oder Deepfakes – zufügen (könnten).[451] Die weiteren Tatbestandsmerkmale des Art 5 Abs 1 lit a KI-VO müssen diesbezüglich nicht vorliegen.

Das absolute Verbot einer Verhaltensmanipulation gem Art 5 Abs 1 lit a KI-VO ist dagegen in mehrfacher Hinsicht beschränkt worden. An erster Stelle wird nicht die Entwicklung solcher KI-Systeme verboten, sondern bloß das Inverkehrbringen, die Inbetriebnahme und die Verwendung. Überdies müssen manipulative oder täuschende Techniken „*absichtlich*" eingesetzt worden sein, um eine Verhaltensänderung zu bewirken.[452] Diese Absicht wird jedoch nicht vermutet, wenn die Beeinflussung auf Faktoren zurückzuführen ist, die nicht Teil des KI-Systems sind und außerhalb der Kontrolle des Anbieters oder Betreibers liegen (ErwGr 29 KI-VO). Weder der Anbieter noch der Betreiber kannten diese Faktoren und mussten diese auch nicht vernünftigerweise vorhersehen oder vermindern. Es besteht immerhin keine zwingende Notwendigkeit dafür, dass der Anbieter oder Betreiber durch den gezielten Einsatz solcher Techniken ebenfalls die Absicht hat, einen erheblichen Schaden zuzufügen. Dennoch gibt es berechtigte Kritik daran, dass das Verbot durch dieses subjektive Element stark verwässert wird.[453] Ein KI-System, das in der Lage ist, erhebliche Manipulationen zu bewirken, ist unabhängig davon besonders gefährlich, ob der Anbieter oder Betreiber diesen Effekt beabsichtigt, ihm keine Bedeutung beimisst oder ihn sogar innerlich ablehnt.[454] Entscheidend sollte dementsprechend vielmehr ein objektives Kriterium sein, das sich auf die „*Eignung*" zur Verhaltensmanipulation konzentriert. Auf diese Weise wären auch Methoden der personalisierten Werbung ohne bedeutende verhaltenssteuernde Effekte akzeptabel und mit dem Verhältnismäßigkeitsgrundsatz konform.[455] Dies entkräftet zudem die Befürchtung, dass das Geschäftsmodell der personalisierten Werbung ansonsten „*vor dem Aus stünde*",[456] sodass personalisierte Werbung mE durchaus vom Verbot erfasst sein könnte.[457]

Im Fall von OpenAI ist GPT-4o wohl ein GPAI-Modell und die Browseranwendung ChatGPT ein KI-System; vgl *Bomhard/Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, 45 (50).

451 Dafür spricht mE auch Art 5 Abs 8 KI-VO, wonach „*Art 5 nicht die Verbote [berührt], die gelten, wenn KI-Praktiken gegen andere Rechtsvorschriften der Union verstoßen*"; vgl auch ErwGr 45 KI-VO: „*Praktiken, die nach Unionsrecht, einschließlich Datenschutzrecht, Nichtdiskriminierungsrecht, Verbraucherschutzrecht und Wettbewerbsrecht, verboten sind, sollten von der KI-VO nicht betroffen sein*."

452 *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 26.

453 *Ebert/Spiecker*, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188 (1189).

454 *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 4.

455 *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 5.

456 *Bomhard/Merkle*, Europäische KI-Verordnung, RDi 2021, 276 (279).

457 Krit *Bomhard/Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, 45 (Rz 13); *Hafner-Thomic*, Personalisierte Preise im Online-Handel (2024) 154 (Fn 908).

Die Begrenzung auf wesentliche Verhaltensänderungen schwächt das Verbot ohnehin zusätzlich ab. „*Wesentlich*“ wird ein Verhalten verändert, indem die Fähigkeit einer Person oder Personengruppe, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte und ihr bzw ihnen dadurch ein „*erheblicher Schaden*“ (mit hinreichender Wahrscheinlichkeit) zugefügt wird. In Betracht kommen nunmehr auch finanzielle Nachteile (inkl unerwünschte Vertragsabschlüsse)[458] – abseits von physischen und psychischen Schäden[459] – welche sich im Laufe der Zeit auch anhäufen können (ErwGr 29 KI-VO). Ab wann von einer konkreten Erheblichkeit eines zugefügten Schadens auszugehen ist (zB durch die Angabe einer Wertgrenze bzw einer Bagatellausnahme), wird in der KI-VO nicht näher erläutert.

3.2.2 Verhaltensmanipulation iSv Art 5 Abs 1 lit b KI-VO

Verboten ist „*das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung ausnutzt, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird*.“

Dieses Verbot zielt darauf ab, bestimmte Personen oder Personengruppen zu schützen, die besonders anfällig für manipulative KI-Techniken sein könnten. Aufgrund ihres Alters (zB Kinder oder ältere Menschen), einer geistigen Behinderung oder ihrer sozialen oder wirtschaftlichen Situation – etwa Personen, die in extremer Armut leben, und ethnische oder religiöse Minderheiten (vgl ErwGr 29 KI-VO) – könnten diese umso mehr „*zum bloßen Objekt des*

[458] *Valta/Vasel*, Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz, ZRP 2021, 142 (143); aA *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 27: Der Autor interpretierte aber noch den ursprünglichen Entwurf der KI-VO.

[459] *Fülöp*, AI Act: Das Ende europäischer Innovation oder Gefahr für den Datenschutz? - eine Relativierung, Dako 2023/42, 82 (82): Manipulative Techniken und unterschwellige Beeinflussung können psychische Probleme verursachen.

Gewinnstrebens oder sonstiger Interessen desjenigen degradiert [werden], der das KI-System zum Einsatz bringt."[460]

Ein Unterschied zum Verbot gem Art 5 Abs 1 lit a KI-VO ist das geschützte Rechtsgut. Während hier va die „*unterschwellige*" Beeinflussung im Mittelpunkt steht, verbietet Art 5 Abs 1 lit b KI-VO die Ausnutzung von „*Schwäche bzw Schutzbedürftigkeit*". Dies kann sogar dann zutreffen, wenn sich die Person der Einflussnahme auf ihre Willensbildung bewusst ist, jedoch aufgrund ihrer persönlichen Eigenschaften (zB Alter oder geistige Behinderung) oder ihrer sozialen (zB Einsamkeit) und wirtschaftlichen Stellung (zB Armut) keine ausreichende Gegenwehr leisten kann.[461] Häufig wird davon ausgegangen, dass gezielte Werbung keine nennenswerten Auswirkungen auf Menschen hat. Dies kann jedoch der Fall sein, wenn zB die Schwachstellen einer Person für erfolgreiche Werbung genutzt werden.[462] Das ist besonders im Hinblick auf Menschen aus benachteiligte Gruppen relevant, die möglicherweise nicht wissen, dass sie sich gegen (Direkt-)Marketing entscheiden können oder dass sie ein Mitspracherecht haben, wenn Entscheidungen automatisiert werden.[463] Im Kontext des Verbraucherverhaltens stellt die Ausnutzung individueller Schwächen, wie bspw stark ausgeprägte Neigungen oder Abhängigkeiten, die durch umfangreiche Datenerfassung und Profiling offenbart werden, ein wachsendes Problem dar.[464]

3.3 Verbot des Social Scoring

Es ist erfreulich, dass die ursprüngliche Formulierung in Art 5 Abs 1 lit c KI-VO – nach zahlreicher Kritik[465] – gestrichen wurde, die besagte, dass das Verbot sozialer Bewertungen mittels

[460] *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 9.

[461] *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 8.

[462] Ein Kind, das ein Spielzeug verwendet, welches mit einem Sprachassistenzsystem verbunden ist, könnte mE leichter beeinflussbar sein, wenn es personalisierte Empfehlungen erhält, zB zum Kauf bestimmter Produkte. Art 6 Abs 1 KI-VO (produktbezogene Hochrisiko-KI) wäre mE in einem solchen Fall gerade nicht einschlägig; vgl *Wichering*, Die Woche im Blick, BB 2023, 2945 (2945): ein mit einem Voicebot ausgestattetes Spielzeug kann zu gefährlichem Verhalten verleiten.

[463] EU-Grundrechteagentur, Getting the future right – Artificial Intelligence and Fundamental Rights Report (2020) 64, abrufbar unter <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_ en.pdf> (2.5.2024).

[464] *Wendehorst* 14.12.2021, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective, 16, abrufbar unter <https://www.sozialministerium.at/Themen/Konsumentenschutz/Konsumentenpolitik.html> (8.5.2024).

[465] *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, 528 (530); *Linardatos*, Auf dem Weg zu einer europäischen KI-Verordnung,

KI-Systemen[466] nur für „*Behörden oder in deren Auftrag*“ gelte. Dadurch erstreckt sich dieses nun sowohl auf den staatlichen als auch auf den privaten Sektor,[467] in welchem „*die Dystopie solcher Systeme [...], zB bei Vertragsabschlüssen oder dem Zugang zu Dienstleistungen, viel näher [liegt]*.“[468] KI-Systeme, die eine derartige soziale Bewertung natürlicher Personen durch öffentliche oder private Akteure bereitstellen, können zu diskriminierenden Ergebnissen und zur Ausgrenzung bestimmter Gruppen führen (ErwGr 31 KI-VO). Die genannten Beispiele SCHUFA und AMAS[469] verdeutlichen die potenziellen Gefahren, die von solchen Systemen ausgehen können.

Dennoch wirft diese Regelung weiterhin erhebliche Unsicherheiten auf, sodass sich ihre praktische Bedeutung und Wirksamkeit noch herausstellen müssen. Genauer gesagt ist das Verbot nur dann anwendbar, wenn die soziale Bewertung zu einer der beiden folgenden Konsequenzen führt: (i) eine „*Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden*“, oder (ii) eine „*Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist*."[470] Ausdrücklich nicht erfasst sind rechtmäßige Praktiken zur Bewertung natürlicher Personen, die im Einklang mit dem Unionsrecht und dem nationalen Recht zu einem bestimmten Zweck durchgeführt werden (ErwGr 31 KI-VO). In vielen Fällen wird daher eine Interessenabwägung durchzuführen sein,[471] wodurch das Risiko einer Verbotsumgehung signifikant steigt und das „*Recht auf Anonymität und die*

GPR 2022, 58 (61); EDSA/EDSB 18.6.2021, Gemeinsame Stellungnahme 5/2021, Rz 29: Es sind hauptsächlich Privatunternehmen, etwa Anbieter von sozialen Medien und Cloud-Diensten, in der Lage, enorme Mengen personenbezogener Daten zu verarbeiten und Social Scoring vorzunehmen.

[466] Hierbei werden natürliche Personen oder Gruppen natürlicher Personen durch KI-Systeme in einem bestimmten Zeitraum auf der Grundlage zahlreicher Datenpunkte in Bezug auf ihr soziales Verhalten in verschiedenen Zusammenhängen oder aufgrund bekannter, vermuteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale bewertet oder klassifiziert (ErwGr 31 KI-VO).

[467] Absolut verboten ist „*das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale*“ (Art 5 Abs 1 lit c KI-VO).

[468] *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 12.

[469] Vgl Kapitel 2.7.3 (Scoring).

[470] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 29.

[471] *Spindler*, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E), CR 2021, 361 (365).

Privatsphäre durch Social Scoring ausgehöhlt oder sogar unmöglich gemacht [wird].“[472] Der Wortlaut „*über einen bestimmten Zeitraum*“ wirft weitere Fragen auf. Es bleibt unklar, ob einmalige Social-Scoring-Aktivitäten zulässig sind – die sich nebenbei bemerkt über eine beträchtliche Zeitspanne erstrecken können – oder ob das Verbot erst für wiederholte Einsätze solcher Praktiken gilt.[473]

Zumindest werden KI-Systeme, die dazu bestimmt sind, über den Zugang und die Bereitstellung bestimmter grundlegender privater sowie öffentlicher Dienste und Leistungen zu entscheiden, als Hochrisiko-KI eingestuft (Art 6 Abs 2 KI-VO iVm Anhang III Z 5 KI-VO). Hierzu gehören auf jeden Fall Kreditwürdigkeitsprüfungen und Bonitätsbewertungen natürlicher Personen sowie Risikobewertungen und Preisgestaltungen im Bereich von Kranken- und Lebensversicherungen (vgl auch ErwGr 58 KI-VO).

Betreiber solcher Systeme sind vor dem erstmaligen Einsatz dazu verpflichtet, eine neue Form der Risikominimierung durchzuführen, nämlich die sog „*Grundrechte-Folgenabschätzung*“ (Art 27 KI-VO). Diese Pflicht besteht parallel zur Durchführung einer DSFA und hat zum Ziel, dass der Betreiber die spezifischen Risiken für die Rechte von Einzelpersonen oder Gruppen von Einzelpersonen identifiziert, die voraussichtlich betroffen sind. Dabei sollen Maßnahmen ermittelt werden, die bei Eintritt dieser Risiken zu ergreifen sind (vgl ErwGr 96 KI-VO).

3.4 Biometrische Identifizierung

3.4.1 Verbot ungezielten Auslesens von Gesichtsbildern aus dem Internet

Obwohl Art 5 Abs 1 lit e KI-VO auf den ersten Blick für Werbetreibende nicht unmittelbar relevant erscheint, ist es dennoch wichtig, ihn iZm dem Datenschutzaspekt dieser Abhandlung sowie den allgemeinen Herausforderungen von Big Data-Analysen zu erwähnen. Die brisanten

[472] Deutscher Anwaltverein 25.11.2021, Stellungnahme Nr 57/2021, 9, abrufbar unter <https://anwaltverein.de/de/newsroom/sn-57-21-ki-verordnungsvorschlag-der-eu-kommission> (30.4.2024).

[473] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 31.

Vorgehensweisen von Unternehmen wie PimEyes[474] und Clearview AI[475] veranschaulichen die Notwendigkeit eines Verbots – auch für den Privatsektor[476] – von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Sammeln von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern („*Scraping*"; vgl auch ErwGr 119 KI-VO).[477] Ebenso sind die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung verboten, „*da dies das Gefühl der Massenüberwachung verstärkt und zu schweren Verstößen gegen die Grundrechte, einschließlich des Rechts auf Privatsphäre, führen kann*" (ErwGr 43 KI-VO).

3.4.2 Emotionserkennung

Die Verwendung von Emotionserkennungssystemen ist va für soziale Netzwerke attraktiv, da die Erfassung von Emotionsdaten ihrer Nutzer vielversprechende Möglichkeiten in Bezug auf die Erstellung von Nutzerprofilen[478] und die Personalisierung von Werbung bietet.[479]

„*Emotionserkennungssysteme*" sind KI-Systeme, die dem Zweck dienen, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten[480] festzustellen oder daraus abzuleiten (Art 3 Z 39 KI-VO). Dies beinhaltet ua die Emotionen oder Absichten wie Glück, Trauer, Wut, Überraschung, Ekel, Verlegenheit, Aufregung, Scham, Verachtung, Zufriedenheit und Vergnügen (ErwGr 18 KI-VO). Physische Zustände (zB Schmerz oder Ermüdung) sollen diesem Begriffsverständnis nicht unterliegen. Ebenfalls sind darunter grds nicht die bloße Erkennung offensichtlicher Ausdrucksformen (zB einfache Gesichtsausdrücke wie

---

[474] PimEyes ist eine Suchmaschine, die öffentlich zugängliche Bilder im Internet nach biometrischen Merkmalen scannt, insb nach Gesichtern, und die erfassten Informationen in einer Datenbank speichert; vgl LfDI Baden-Württemberg, Bußgeldverfahren wegen Massenspeicherung von biometrischen Daten aus Gesichtsscan, ZD-Aktuell 2023, 01016 (beck-online).

[475] Clearview AI betreibt eine Biometriedatenbank und sammelt dafür Bilder sowie Videos aus öffentlich zugänglichen Quellen; vgl *Qasim*, Italien: Kein Freifahrtschein für Gesichtserkennungssoftware - Bußgeld iHv 20 Mio. EUR gegen Clearview AI, ZD-Aktuell 2022, 01144 (beck-online); *Vilain*, Speech by Zoé Vilain - Digital Rights and Corporate Accountability: Lessons from Clearview AI and ChatGPT, AnwBl 2024/145, 284 (284).

[476] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 35.

[477] DSB 9.5.2023, D130.703 (2022-0.277.156): Die DSB stellte fest, dass Clearview AI als Verantwortlicher biometrische Daten iSd Art 9 Abs 1 DSGVO unrechtmäßig verarbeitet hat. Selbst wenn Art 9 DSGVO nicht anwendbar wäre, würde die Verarbeitung unrechtmäßig iSd Art 6 Abs 1 DSGVO erfolgen. Darüber hinaus wurden die Grundsätze für die Datenverarbeitung gem Art 5 Abs 1 lit a, b und c DSGVO verletzt.

[478] *Zuboff*, Das Zeitalter des Überwachungskapitalismus (2019) 329.

[479] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 48.

[480] Diese ermöglichen auch die Erkennung von Emotionen natürlicher Personen (ErwGr 14 KI-VO), wodurch ua eine biometrische Identifizierung realisiert werden kann (ErwGr 15 KI-VO).

ein Stirnrunzeln oder ein Lächeln sowie Stimmmerkmale wie eine erhobene Stimme oder ein Flüstern), Gesten und Bewegungen (zB Hand-, Arm- oder Kopfbewegungen) zu verstehen, außer diese werden zum Erkennen oder Ableiten von Emotionen verwendet. Das unmittelbare Auslesen von Texten oder die Auswertung von sog „*Emotionsbuttons*" fallen gleichfalls nicht unter den Begriff der biometrischen Daten.[481]

Dagegen gibt es berechtigte Bedenken,[482] insb weil sich Gefühlsausdrücke je nach Kultur oder Situation stark unterscheiden können, sogar bei derselben Person. Ein Hauptproblem solcher Systeme ist ihre begrenzte Zuverlässigkeit, Unklarheit und begrenzte Verallgemeinerbarkeit. Daher können KI-Systeme, die Emotionen oder Absichten anhand biometrischer Daten erkennen oder ableiten, diskriminierende Ergebnisse liefern und in die Rechte und Freiheiten der betroffenen Personen eingreifen (ErwGr 44 KI-VO).

In Anbetracht dessen unterscheidet die KI-VO zwischen zwei Ansätzen zur Regulierung von Emotionserkennungssystemen: Erstens sind Systeme, die darauf abzielen, Emotionen am Arbeitsplatz und in Bildungseinrichtungen abzuleiten, grds verboten (Art 5 Abs 1 lit f KI-VO iVm ErwGr 44 KI-VO). Zweitens gelten alle anderen Systeme als hochriskant (Art 6 Abs 2 KI-VO iVm Anhang III Z 1 lit c KI-VO, ErwGr 54 KI-VO). Zusätzlich normiert Art 50 Abs 3 KI-VO eine ausdrückliche Transparenzpflicht,[483] wonach Betreiber eines Emotionserkennungssystems die davon betroffenen natürlichen Personen über den Betrieb des Systems spätestens zum Zeitpunkt der ersten Interaktion in barrierefreier, klarer und eindeutiger Weise informieren müssen (vgl Art 50 Abs 5 KI-VO). Natürlichen Personen ist mitzuteilen, dass sie KI-Systemen ausgesetzt sind, die durch die Verarbeitung ihrer biometrischen Daten die Gefühle oder Absichten dieser Personen identifizieren, ableiten oder sie bestimmten Kategorien zuordnen können (ErwGr 132 KI-VO).

Weiters dürfen personenbezogene Daten nur gem der DSGVO verarbeitet werden, denn die Tatsache, dass ein KI-System gem der KI-VO als ein Hochrisiko-KI-System eingestuft wird, sollte

---

[481] *Kalbhenn*, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, 663 (670).

[482] *Veale/Borgesius*, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97 (107 f).

[483] *Geroldinger* in *Österreichischer Juristentag* (Hrsg), Verhandlungen des Einundzwanzigsten Österreichischen Juristentages Wien 2022 II/2 (2022) 111.

nicht dahin gehend ausgelegt werden, dass dessen Verwendung nach anderen Rechtsakten der EU oder nach nationalen Rechtsvorschriften, die mit dem Unionsrecht vereinbar sind, rechtmäßig ist, bspw in Bezug auf den Schutz personenbezogener Daten, die Verwendung von Lügendetektoren und ähnlichen Instrumenten oder anderen Systemen zur Ermittlung des emotionalen Zustands natürlicher Personen (ErwGr 63 KI-VO).

Es ist beachtlich, dass Affective Computing-Systeme aufgrund ihrer praktischen Relevanz und ihres hohen Gefahrenpotenzials[484] nunmehr angemessen in der KI-VO berücksichtigt wurden.[485] Letztlich hat die KI-VO ihren Fokus eindeutig auch auf den Schutz der Grundrechte gelegt[486] und sich nicht ausschließlich von der Produktsicherheit leiten lassen.[487]

3.4.3 Biometrische Echtzeit-Fernidentifizierung

Art 5 Abs 1 lit h KI-VO untersagt (nur) die Verwendung – und zB nicht das Inverkehrbringen und die Inbetriebnahme – „*biometrischer Echtzeit-Fernidentifizierungssysteme*“[488] in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (vgl auch Art 5 Abs 2-6 KI-VO iVm ErwGr 32 ff KI-VO). Für die Analyse der Auswirkungen der KI-VO auf den Marketingbereich ist dieses Verbot daher nebensächlich. Außerdem gilt dieses Verbot ohnedies für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung (Art 5 Abs 1 lit h UAbs 2 KI-VO), sollte nicht ausnahmsweise ein Erlaubnistatbestand iSd Art 9 Abs 2 DSGVO (insb die ausdrückliche Einwilligung Betroffener) vorliegen.

---

[484] *Stenner*, Emotionale KI: Berechnete Gefühle, abrufbar unter <https://netzpolitik.org/2021/emotionale-ki-berechnete-gefuehle> (2.5.2024).

[485] EDSA/EDSB 18.6.2021, Gemeinsame Stellungnahme 5/2021, Rz 35: Zur Forderung eines gänzlichen Verbots.

[486] Als hochriskant sollten solche KI-Systeme eingestuft werden, die erhebliche schädliche Auswirkungen auf die Grundrechte von Personen in der Union haben (ErwGr 46 letzter Satz KI-VO). Dabei ist das Ausmaß der nachteiligen Auswirkungen auf die durch die GRC geschützten Grundrechte von besonderer Bedeutung (ErwGr 48 KI-VO). Zu diesen Rechten gehören ua die Würde des Menschen, die Achtung des Privat- und Familienlebens, der Schutz personenbezogener Daten, die Nichtdiskriminierung, der Verbraucherschutz und völkerrechtlich garantierte Kinderrechte. Emotionserkennungssysteme haben allein aufgrund ihrer Zweckbestimmung eines hohes Risiko, die Grundrechte zu schädigen (vgl ErwGr 52 KI-VO).

[487] *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 17 f.

[488] Das ist ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und eine Identifizierung grds ohne erhebliche Verzögerung oder aber auch mit begrenzten kurzen Verzögerungen erfolgen (Art 3 Z 42 KI-VO iVm ErwGr 17 KI-VO).

3.4.4 Biometrische Kategorisierung

Unter „*biometrischen Daten*“ versteht die KI-VO alle mit speziellen technischen Verfahren gewonnenen personenbezogenen Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen[489] einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische[490] Daten (Art 3 Z 34 KI-VO). Es soll das gleiche Verständnis dieses Begriffs angewendet werden wie in der DSGVO (ErwGr 14 KI-VO).[491] Abgesehen von der bereits angesprochenen Emotionserkennung, können biometrische Daten zur Authentifizierung,[492] Identifizierung[493] oder Kategorisierung natürlicher Personen beitragen bzw diese erst möglich machen. Konsequenterweise sollen – da biometrische Daten eine besondere Kategorie personenbezogener Daten[494] darstellen – kritische Anwendungsfälle biometrischer Systeme verboten (Art 5 Abs 1 lit g KI-VO) oder wenigstens als hochriskant eingestuft werden (Art 6 Abs 2 KI-VO iVm Anhang III Z 1 KI-VO), sofern ihre Verwendung bzw Verarbeitung (einschließlich Erhebung) nach den einschlägigen Rechtsvorschriften der Union – insb nach der DSGVO – und den nationalen Rechtsvorschriften überhaupt zulässig ist (ErwGr 54 KI-VO). In einer Gesellschaft, in der die Freiheit verfassungsrechtlich verankert ist, ist es ein grundlegendes Prinzip, dass Menschen

[489] Zu diesen Merkmalen gehören ua eine automatische Analyse und/oder Erkennung von menschlichen Merkmalen wie der Körperform, Gangart, Haltung, Herzfrequenz, Blutdruck, Geruch, DNS, Stimme, Prosodie, Haarfarbe, Augenfarbe (Iris/Retina), Augenbewegungen, des charakteristischen Tastenanschlags, oder von Tätowierungen, usw (ErwGr 15 KI-VO). Aber auch persönliche Vorlieben und Interessen (ErwGr 132 KI-VO); vgl *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 22.

[490] Die Daktyloskopie, abgeleitet von den griechischen Wörtern „*daktylos*“ (dt „Finger“) und „*skopein*“ (dt „betrachten“), beschäftigt sich mit den individuellen Merkmalen von Händen und Füßen. Ihr Hauptzweck liegt in der Identifizierung von Personen anhand ihrer einzigartigen Fingerabdrücke.

[491] Biometrische Daten iSd DSGVO sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten (Art 4 Z 14 DSGVO iVm ErwGr 51 DSGVO).

[492] „*Biometrische Verifizierung*“ ist die automatisierte Eins-zu-eins-Verifizierung, inkl Authentifizierung, der Identität natürlicher Personen durch den Vergleich ihrer biometrischen Daten mit zuvor bereitgestellten biometrischen Daten (Art 3 Z 36 KI-VO). Der typische Zweck solcher Verifizierungssysteme besteht darin, zu bestätigen, dass eine bestimmte natürliche Person tatsächlich diejenige ist, für die sie sich ausgibt. Dadurch soll nur diese Person ua in der Lage sein, Zugang zu einem Dienst zu erhalten, ein Gerät zu entsperren oder Sicherheitszugang zu Räumlichkeiten zu erhalten (ErwGr 15 KI-VO).

[493] „*Biometrische Identifizierung*“ ist die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind (Art 3 Z 35 KI-VO), unabhängig davon, ob die Einzelperson ihre Zustimmung dazu gegeben hat oder nicht (ErwGr 15 KI-VO).

[494] Das sind ua die in Art 9 Abs 1 DSGVO angeführten Kategorien personenbezogener Daten (Art 3 Z 37 KI-VO).

das Recht auf informationelle Selbstbestimmung haben und grds selbst entscheiden können, ob sie persönliche Merkmale offenlegen möchten oder nicht.[495]

Für andere Zwecke als die Strafverfolgung ist die Verarbeitung biometrischer Daten grds verboten, vorbehaltlich der in der KI-VO vorgesehenen begrenzten Ausnahmefällen (ErwGr 39 KI-VO). Jedoch muss den nachstehenden Überlegungen vorausgeschickt werden, dass biometrische Daten nur dann als sensible Daten iSd Art 9 Abs 1 DSGVO gelten, wenn sie tatsächlich zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden. Die Einstufung von biometrischen Daten als sensible Daten hängt daher vom konkreten Verarbeitungszweck ab. Dieser Zweck muss darauf abzielen, durch die Verarbeitung selbst eine eindeutige Identifizierung herbeizuführen. Folglich betrifft diese Einstufung nur automatisierte Identifizierungsprozesse. Ein Gesichtsbild einer Person wird zB nur dann ein sensibles Datum iSd DSGVO sein, wenn es mit einem Gesichtserkennungsalgorithmus verarbeitet wird.[496]

Verboten sind nun das Inverkehrbringen, die Inbetriebnahme (lediglich) für diesen spezifischen Zweck oder die Verwendung von „*Systemen zur biometrischen Kategorisierung*“,[497] mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten (Art 5 Abs 1 lit g KI-VO).[498] Ausgenommen sind aber solche biometrischen Kategorisierungssysteme, bei denen es sich um eine reine Nebenfunktion handelt, welche untrennbar mit einem anderen kommerziellen Dienst verbunden ist.[499] Bspw könnten Filter zur Kategorisierung von Gesichts- oder Körpermerkmalen, die auf Online-Marktplätzen verwendet werden, eine solche Nebenfunktion darstellen. Diese Filter können ausschließlich iZm der Hauptdienstleistung verwendet werden, die darin besteht, ein

---

[495] *Rostalski/Weiss* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 3 Rz 22.

[496] *Feiler/Forgó*, EU-DSGVO und DSG[2] (2022) Art 9 Rz 6.

[497] Ein „*System zur biometrischen Kategorisierung*“ ist ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien zuzuordnen, sofern es sich um eine Nebenfunktion eines anderen kommerziellen Dienstes handelt und aus objektiven technischen Gründen unbedingt erforderlich ist (Art 3 Z 40 KI-VO).

[498] Nur im Bereich der Strafverfolgung dürfen rechtmäßig erworbene biometrische Datensätze gekennzeichnet, gefiltert und kategorisiert werden.

[499] Dh die Funktion kann aus objektiven technischen Gründen nicht ohne den Hauptdienst verwendet werden und die Integration dieses Merkmals oder dieser Funktion dient nicht dazu, die Anwendbarkeit der Vorschriften der KI-VO zu umgehen (ErwGr 16 KI-VO).

Produkt zu verkaufen. Sie ermöglichen es dem Verbraucher, zu sehen, wie das Produkt an seiner Person aussieht, und helfen ihm so, eine Kaufentscheidung zu treffen (ErwGr 16 KI-VO). Solange die Verarbeitung biometrischer Daten gem den Bestimmungen der DSGVO rechtmäßig erfolgt, die Datenverarbeitungsgrundsätze eingehalten werden und kein verbotenes Nudging und kein unzulässiger Einsatz von Dark Patterns gem Art 5 Abs 1 lit a oder b KI-VO (Verhaltensmanipulation) vorliegt, ist mE tatsächlich von einer prinzipiellen Unbedenklichkeit derartiger Filtersysteme auszugehen.

Als Hochrisiko-KI gelten dagegen die folgenden Biometrie-Systeme (Art 6 Abs 2 KI-VO iVm Anhang III Z 1 KI-VO): (a) „*biometrische Fernidentifizierungssysteme*“[500] (außer biometrische Verifizierungssysteme),[501] und (b) KI-Systeme, die „*bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet*“ werden sollen, soweit sie nicht nach der KI-VO verboten sind (ErwGr 54 KI-VO).

3.5 Die Entscheidungsfindung nur unwesentlich beeinflussende KI-Systeme

Die KI-VO führt in ihrem ErwGr 53 aus, dass es auch „*KI-Systeme, die das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflussen*“ gibt. Diese hätten keine Auswirkungen auf den Inhalt und damit das Ergebnis der Entscheidungsfindung. Es fehlt aus diesem Grund ein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen (Art 6 Abs 3 KI-VO).

Es kommt zudem nicht darauf an, ob es sich um eine menschliche oder automatisierte Entscheidung handelt. Dementsprechend sollen Systeme, die zwar auf der Hochrisiko-Liste des Anhang III stehen, aber mind eine der folgenden Alternativbedingungen erfüllen, doch nicht als hochriskant gelten: (a) das System ist dazu bestimmt, in einem Verfahren eine eng gefasste

[500] Das ist ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und idR aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren (Art 3 Z 41 KI-VO iVm ErwGr 17 KI-VO). Für solche Systeme gelten spezielle inhaltliche Anforderungen bzgl der Protokollierungspflicht (Art 12 Abs 3 KI-VO) und verschärfte Bestimmungen iZm der menschlichen Aufsicht (Art 14 Abs 5 KI-VO).

[501] Technische Ungenauigkeiten von KI-Systemen, die für die biometrische Fernidentifizierung natürlicher Personen bestimmt sind, können nämlich zu verzerrten Ergebnissen führen und eine diskriminierende Wirkung haben (ErwGr 54 KI-VO).

und begrenzte Aufgabe zu erfüllen (zB die Umwandlung unstrukturierter Daten in strukturierte Daten, die Einordnung eingehender Dokumente in Kategorien und die Erkennung von Duplikaten unter einer großen Zahl von Anwendungen), (b) das System verbessert nur eine zuvor abgeschlossene menschliche Tätigkeit bzw ergänzt die menschliche Tätigkeit bloß durch eine zusätzliche Ebene (zB es verbessert nur die in einem bereits verfassten Dokument verwendete Sprache – etwa den professionellen Ton – oder passt den Text nur an einen bestimmten mit einer Marke verbundenen Stil an), (c) das System soll lediglich Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern erkennen, und/oder (d) das System ist dazu bestimmt, eine Aufgabe auszuführen, die eine Bewertung nur vorbereitet, die für die Zwecke der gelisteten Hochrisiko-KI relevant ist (zB die Übersetzung von Erstdokumenten oder die Bearbeitung von Dossiers, wozu verschiedene Funktionen wie Indexierung, Suche, Text- und Sprachverarbeitung oder Verknüpfung von Daten mit anderen Datenquellen zählen).[502]

Solche KI-Systeme können bzw sollen in verschiedenen Bereichen unterstützende Funktionen übernehmen und bieten demgemäß „*interessante Gestaltungsmöglichkeiten*".[503] Mithilfe dieser Technologien können große Datenmengen schnell und präzise analysiert werden. Unternehmen können dadurch wichtige Erkenntnisse gewinnen und fundierte Entscheidungen treffen. Durch die KI-gestützte Auswertung des Kundenverhaltens können Werbetreibende – wie schon bei Cookies – Trends und Muster erkennen, personalisierte Marketingstrategien und Werbekampagnen entwickeln sowie entsprechend anpassen.[504]

Die mögliche übermäßige Begeisterung von Marketingabteilungen angesichts dieser Befreiung von den üblichen Verpflichtungen für Hochrisiko-KI wird mE durch zwei Einschränkungen deutlich relativiert: Zum einen gilt ein KI-System, das Profiling gem der DSGVO beinhaltet, auf jeden Fall als hochriskant (Art 6 Abs 3 UAbs 2 KI-VO). Zum anderen muss ein Anbieter bereits im Vorfeld Transparenz gewährleisten, indem er dokumentiert, warum er der Ansicht ist, dass ein KI-System unter den genannten Bedingungen gerade kein hohes Risiko darstellt, bevor

[502] EK 12.12.2023, Künstliche Intelligenz – Fragen und Antworten, 3.

[503] *Bomhard/Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, 45 (Rz 17).

[504] *Isler*, KI-Gestützte Entscheidungsfindung: Wie Geschäftsführer von Künstlicher Intelligenz profitieren können, abrufbar unter <https://www.hagel-it.de/it-insights/ki-gestuetzte-entscheidungsfindung-wie-geschaeftsfuehrer-von-kuenstlicher-intelligenz-profitieren-koennen.html> (2.5.2024).

dieses System in Verkehr gebracht oder in Betrieb genommen wird. Diese Dokumentation muss der Anbieter zwar nur auf Anfrage den zuständigen nationalen Behörden zur Verfügung stellen, aber das KI-System selbst muss in der EU-Datenbank für Hochrisiko-KI (Art 71 KI-VO) registriert werden (Art 6 Abs 4 KI-VO iVm Art 49 Abs 2 KI-VO).

Betreiber laufen daher Gefahr, dass der Anbieter eine (bewusste) Fehleinschätzung seines KI-Systems vorgenommen hat und sie daher Hochrisiko-KI verwenden, ohne die dafür vorgesehenen Pflichten zu beachten.[505] In solchen Fällen können gegen den Anbieter empfindliche Geldbußen[506] verhängt werden (Art 80 Abs 7 KI-VO iVm Art 99 Abs 4 KI-VO). Auch Betreiber von Hochrisiko-KI-Systemen iSd Anhang III, die natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen unterstützen, können Geldbußen erhalten, wenn sie die betroffenen Personen nicht darüber informieren, dass diese Gegenstand des Einsatzes eines solchen Hochrisiko-KI-Systems sind (Art 26 Abs 11 KI-VO iVm Art 99 Abs 4 lit e KI-VO). Selbstverständlich müssen Anbieter und Betreiber – ebenfalls unter Androhung von Geldbußen – ihre allgemeine Informationspflicht einhalten (Art 50 KI-VO iVm Art 99 Abs 4 lit g KI-VO).

Es ist für Unternehmen keinesfalls ratsam, dieses Risiko einzugehen und die obengenannten Bestimmungen (schuldhaft) zu umgehen, wenn sie zB Biometrik- oder bestimmte Social-Scoring-Systeme anbieten oder verwenden wollen.

3.6 KI-Systeme mit geringem Risiko

Grds sind KI-Systeme, die im Rahmen von Marketing oder der Marktforschung eingesetzt werden, weder untersagt (Art 5 KI-VO) noch hochriskant (Art 6 ff KI-VO).[507] Dh jedoch nicht, dass solche Systeme völlig unabhängig von der KI-VO eingesetzt werden können.[508] Unternehmen, die va Chatbots[509] verwenden, um Kaufempfehlungen abzugeben, Anfragen ihrer Kunden zu

[505] *Ammann/Pohle*, KI-Verordnung – Was bisher geschah und jetzt zu tun ist, CB 2024, 137 (140).

[506] Höchstens 15 Mio Euro oder – im Falle von Unternehmen – 3 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (Art 99 Abs 4 KI-VO). Bei falschen, unvollständigen oder irreführenden Informationen drohen Geldbußen bis max 7,5 Mio Euro oder – im Falle von Unternehmen – von bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (Art 99 Abs 5 KI-VO).

[507] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 81.

[508] Abgesehen von der Möglichkeit, sich freiwilligen Verhaltenskodizes zu unterwerfen (vgl Art 95 KI-VO); vgl *Bisset*, KI Compliance (Stand 17.1.2024, Lexis Briefings in lexis360.at).

[509] Innerhalb sozialer Netzwerke (Social Media) werden auch sog „*Social Bots*“ eingesetzt, die für das algorithmusbasierte Teilen, Liken oder Kommentieren von Beiträgen eingesetzt werden. Allerdings werden sie

beantworten oder sonstige Konversationen zu betreiben,[510] unterliegen den spezifischen Anforderungen zur Transparenz und Kennzeichnung gem Art 50 KI-VO.[511]

3.6.1 Kennzeichnung von interaktiven KI-Systemen

Anbieter von KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, müssen so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen – spätestens zum Zeitpunkt der ersten Interaktion (Art 50 Abs 5 KI-VO) – in barrierefreier, klarer und eindeutiger Weise informiert werden, dass diese mit einem KI-System interagieren (Art 50 Abs 1 KI-VO),[512] da solche Systeme zumindest ein gewisses Risiko in Bezug auf Identitätsbetrug oder Täuschung bergen (ErwGr 132 KI-VO).[513]

Ist es aus der Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich, dass sie es mit einem KI-System zu tun hat, gilt diese Pflicht aber nicht.[514] Die KI-VO selbst legt nicht fest, wann diese Offensichtlichkeit anzunehmen ist, sondern betont, dass die „*Umstände und der Kontext der Nutzung*" entscheidend sind. Folglich ist zu befürchten, dass Anbieter in der Praxis regelmäßig argumentieren, dass eine solche Offensichtlichkeit gegeben ist.[515] Dem ist zu entgegnen, dass bereits jetzt Teile der Bevölkerung solche Systeme nicht von menschlicher Interaktion unterscheiden können.[516] Es fällt vielen Menschen überdies schwer, zwischen

häufiger mit „*Fake Accounts*" und der Verbreitung von „*Fake News*" in Verbindung gebracht; vgl BSI, Exkurs: Social Bots und Chatbots, abrufbar unter <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html> (3.5.2024).

[510] *Bastians* in *Steinrötter* (Hrsg) Europäische Plattformregulierung (2023) § 21 Rz 43.

[511] *Kalbhenn*, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme, ZUM 2021, 663 (669): Nicht gekennzeichnete Chatbots bzw Social Bots verstoßen ua auch gegen den DSA, da sie als „*illegale Inhalte*" gelten; vgl auch ErwGr 120, 136 KI-VO sowie Art 2 Abs 5 KI-VO: „*Die Anwendung der Bestimmungen über die Haftung der Anbieter von Vermittlungsdiensten [(Art 4 ff DSA)] bleibt [...] unberührt*" (vgl auch ErwGr 11 KI-VO).

[512] *Blawert*, "Transparenz" nach der DSGVO und der KI-VO-E - Ein Rechtsvergleich mit Empfehlungen zur Umsetzung, DSB 2023, 115 (115): Den Betroffenen sollte die Möglichkeit gegeben werden, zu entscheiden, ob ihre Daten mithilfe eines KI-Systems verarbeitet werden sollen oder nicht.

[513] Bei der Erfüllung dieser Verpflichtung sollten die Eigenschaften von Individuen, die aufgrund ihres Alters oder einer Behinderung schutzbedürftigen Gruppen angehören, berücksichtigt werden, sofern das KI-System auch mit diesen Gruppen interagieren soll (ErwGr 132 KI-VO).

[514] *Engelmann/Brunotte/Lütkens*, Regulierung von Legal Tech durch die KI-Verordnung, RDi 2021, 317 (321).

[515] *Bastians* in *Steinrötter* (Hrsg) Europäische Plattformregulierung (2023) § 21 Rz 43.

[516] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 43.

verschiedenen Kommunikationsabsichten wie Werbung, Information, Desinformation und Meinung zu unterscheiden.[517]

Dass die KI-VO weiters zur konkreten Form und zum konkreten Inhalt dieser „*klaren und eindeutigen*" Information schweigt, sorgt in diesem Zusammenhang nicht für die nötige Rechtssicherheit. Ein Hinweis oder eine Kennzeichnung iSd Art 50 Abs 2 KI-VO (iVm ErwGr 133 KI-VO) wird aus systematischen Überlegungen diesbezüglich wohl genügen.[518]

Für Betreiber gilt diese Pflicht nicht.[519] Jedoch gelten für diese andere Transparenzpflichten, die im Unionsrecht oder dem nationalen Recht festgelegt sind (Art 50 Abs 6 KI-VO). Zu denken sei in dieser Hinsicht etwa an die Informationspflichten gem Art 13 f DSGVO, die allerdings grds keine Kennzeichnungspflicht beinhalten. Einzig für vollständig automatisierte nachteilige Entscheidungen im Einzelfall (Art 22 DSGVO) besteht eine datenschutzrechtlich umfassendere Informationspflicht (Art 13 Abs 2 lit f DSGVO: in Bezug auf das „*Ob*" und „*Wie*" dieser Entscheidungsfindung).[520] Für teilautomatisierte Entscheidungen, die (noch) den Großteil der heute eingesetzten KI-Systeme ausmachen, sieht die DSGVO jedoch keine solche Transparenzpflicht vor.[521]

3.6.2 Kennzeichnung von KI-Output

Anbieter von KI-Systemen (inkl GPAI), die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, müssen sicherstellen, dass diese Ergebnisse in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind (Art 50 Abs 2 KI-VO). Eine Fülle von KI-Systemen ist nämlich in der Lage, große Mengen synthetischer Inhalte zu generieren, was es für Menschen zunehmend schwierig macht, diese von menschlich

[517] *Meßmer/Sängerlaub/Schulz*, „Quelle: Internet"? Digitale Nachrichten- und Informationskompetenzen der deutschen Bevölkerung im Test, Studie März 2021, 4, abrufbar unter <https://www.stiftung-nv.de/sites/default/files/studie_quelleinternet.pdf> (3.5.2024).

[518] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 38.

[519] Eine eindeutige Differenzierung zwischen Anbietern und Betreibern ist nicht immer möglich, und in Zukunft werden diese Begriffe wahrscheinlich noch stärker miteinander verschmelzen, weil zunehmend benutzerfreundlichere APIs entwickelt werden; vgl *Veale/Borgesius*, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97 (107).

[520] Vgl Kapitel 2.7.2 (Profiling).

[521] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 129 f: Betroffene haben außerdem nicht das Recht gem der KI-VO, ein System abzulehnen, um stattdessen mit einem Menschen zu kommunizieren.

erzeugten und authentischen Inhalten zu unterscheiden. Die weitreichende Verfügbarkeit und die zunehmenden Fähigkeiten dieser Systeme haben erhebliche Auswirkungen auf die Integrität des Informationsökosystems und das Vertrauen, das ihm entgegengebracht wird. Dies liegt daran, dass neue Risiken iZm Fehlinformationen und Manipulationen in großem Maßstab, Betrug, Identitätsdiebstahl und Verbrauchertäuschungen entstehen (ErwGr 133 KI-VO).

Die Informationen müssen den betreffenden natürlichen Personen erneut spätestens zum Zeitpunkt der ersten Interaktion in klarer und eindeutiger Weise sowie barrierefrei bereitgestellt werden (Art 50 Abs 5 KI-VO). Herausforderungen könnten sich dadurch ergeben, dass die Kennzeichnung in einem „*maschinenlesbaren Format*" erfolgen muss. Es braucht daher integrierte „*technische Lösungen*" (ErwGr 133 KI-VO), welche die Kennzeichnung und die Feststellung ermöglichen, dass die Ausgabe von einem KI-System und nicht von einem Menschen erzeugt oder manipuliert wurde. Diese Techniken und Methoden sollten – sofern technisch möglich – „*hinreichend zuverlässig, interoperabel, wirksam und belastbar*"[522] sein. ErwGr 133 KI-VO nennt demonstrative Beispiele wie Wasserzeichen, Metadatenidentifizierungen, kryptografische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden, Fingerabdrücke oder andere Techniken. Die Techniken sollten je nach Situation auch kombiniert werden.

Grds ist diese Kennzeichnungspflicht durchaus positiv zu bewerten, doch mangelt es erneut an Vorgaben zu einer konkreten Umsetzung. Anbieter könnten evtl versucht sein, die Kennzeichnung in den Metadaten zu „verstecken", sodass nicht davon ausgegangen werden kann, dass eine „*klare*" Information vorliegt. Erstens werden technisch nicht versierte Personen nicht in der Lage sein, diese Informationen vorab einzusehen, geschweige denn diese zu verstehen. Zweitens werden viele Menschen diese aus Unerfahrenheit[523] nicht konsultieren. *Aichinger/Leitner*[524] beschreiben dies völlig richtig: „*Wenn schon von der Maßfigur der durchschnittlichen Internetuser:innen – von der grds kein hoher Kenntnisstand erwartet werden sollte – nicht ausgegangen werden darf, dass diese Maßfigur die Funktionsweise von Cookies*

[522] Anbieter müssen dabei die Besonderheiten und Beschränkungen der verschiedenen Arten von Inhalten, die Umsetzungskosten und den allgemein anerkannten Stand der Technik berücksichtigen (Art 50 Abs 2 Satz 2 KI-VO).

[523] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 60.

[524] *Aichinger/Leitner* in *Mayrhofer/Nessler/Bieber/Fister/Homar/Tumpel* (Hrsg), ChatGPT, Gemini & Co (2024) 175.

und Marketingalgorithmen versteht, bleibt insb fraglich, welchen Kenntnisstand die Maßfigur von durchschnittlichen KI- bzw LLM-User:innen bei noch komplexeren Vorgängen hat oder haben soll – insb auch datenschutzrechtlich." Dadurch droht die Kennzeichnungspflicht mE de facto ins Leere zu laufen.

Für Betreiber gilt diese Kennzeichnungspflicht nicht (vgl wiederum Art 50 Abs 6 KI-VO). Diese Kennzeichnungspflicht gilt überdies nicht, soweit die KI-Systeme lediglich eine unterstützende Rolle bei der Standardbearbeitung ausführen oder die vom Betreiber bereitgestellten Eingabedaten oder ihre Semantik nur unwesentlich verändern (Art 50 Abs 2 Satz 3 KI-VO). Der Begriff „*soweit*"[525] ist meiner Meinung nach nicht mit einem „*wenn*" zu verwechseln bzw gleichzusetzen. Daher besteht keine Kennzeichnungspflicht, wenn ein KI-System lediglich eine unterstützende Funktion bei Standardbearbeitungen erfüllt oder den Input sowie dessen Semantik nur geringfügig verändert. Falls das KI-System jedoch zusätzlich andere Funktionen bietet oder den Input tlw wesentlich und tlw unwesentlich verändert, muss dieser Output mE gekennzeichnet werden („*Teilkennzeichnungspflicht*"). Auch ErwGr 133 KI-VO spricht davon, dass die Kennzeichnungspflicht nicht für KI-Systeme gilt, die „*in erster Linie*" eine unterstützende Funktion für die Standardbearbeitung ausführen bzw die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern.

3.6.3 Kennzeichnung von Deepfakes

Gem Art 3 Z 60 KI-VO ist ein „*Deepfake*" ein durch KI erzeugter oder manipulierter Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde.

Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen nunmehr – spätestens zum Zeitpunkt der ersten Interaktion in

[525] Vgl den englischen Wortlaut von Art 50 Abs 2 Satz 3 KI-VO: „*to the extent*".

barrierefreier, klarer und eindeutiger[526] Weise (Art 50 Abs 5 KI-VO) – offenlegen,[527] dass diese Inhalte künstlich erzeugt oder manipuliert wurden (Art 50 Abs 4 KI-VO).[528] Eine begrenzte Offenlegungspflicht[529] besteht nur, wenn der Inhalt als offensichtlich künstlerisches, kreatives, satirisches, fiktionales oder analoges Werk oder Programm betrachtet wird, um das Recht auf freie Meinungsäußerung und die Freiheit der Kunst und Wissenschaft zu wahren.[530]

Interessant ist mE, dass Betreiber grds keine Offenlegungspflicht für künstlich erzeugte oder manipulierte Texte trifft (Art 50 Abs 4 UAbs 2 KI-VO *e contrario*), und dies gilt selbst dann nicht, wenn es sich um Deepfakes handelt.[531] Betreiber müssen – dem Wortlaut nach – künstlich erzeugte oder manipulierte Texte (bloß) dann „*offenlegen, wenn diese veröffentlicht werden, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren*." Dies soll aber dann nicht gelten, wenn die durch KI „*erzeugten*"[532] „*Inhalte*"[533] menschlich überprüft oder redaktionell kontrolliert wurden und eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt. Diese Ausnahme – vorrangig für journalistische Zwecke – bedeutet, dass der Betreiber – va die Presse bzw (soziale) Medien[534] – den KI-Hintergrund grds nicht offenlegen muss, wenn Inhalte veröffentlicht werden. Diese Ausnahme wirft jedoch Fragen bzgl des Vertrauens der Konsumenten in die Autorenschaft von realen Personen bei Medienveröffentlichungen auf.[535] Journalisten sollten fortlaufend kritisch denken, Fakten verifizieren und den Kontext von Informationen erfassen, um

[526] ErwGr 134 KI-VO meint in klarer und „*deutlicher*" Weise.

[527] Art 50 Abs 4 KI-VO vermisst erneut konkrete Angaben zur Offenlegungsform und zum -inhalt. KI-Output muss nur entsprechend gekennzeichnet und es muss auf seinen künstlichen Ursprung hingewiesen werden (ErwGr 134 KI-VO).

[528] *Kumkar/Rapp*, Deepfakes, ZfDR 2022, 199 (223 ff).

[529] Es muss nur das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offengelegt werden, sodass die Darstellung oder der Genuss des Werks nicht beeinträchtigt wird (Art 50 Abs 4 UAbs 1 Satz 3 KI-VO).

[530] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 58: Es braucht geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter (vgl ErwGr 134 KI-VO).

[531] Allerdings gilt dann wohl Art 50 Abs 2 KI-VO, der ausdrücklich Textinhalte anführt, aber auf der anderen Seite nur Anbieter in die Pflicht nimmt. Betreiber treffen diesbezüglich (bloß) andere Kennzeichnungspflichten nach EU-Recht oder nationalem Recht (Art 50 Abs 6 KI-VO). Zusätzlich sollten Deepfakes mE unter allen Umständen als unlautere Geschäftspraktiken verboten sein, wenn Verbrauchern wirtschaftliche oder finanzielle Schäden durch eine dadurch verursachte Verhaltensmanipulation entstehen (vgl Kapitel 3.2.1).

[532] Die Ausnahme dürfte mE daher nicht auch für „*manipulierte*" Inhalte gelten.

[533] Es ist mE fraglich, ob nur „*Textinhalte*" oder auch „*Bild-, Ton- oder Videoinhalte*" gemeint sind.

[534] *Bomhard/Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, 45 (47): Die Ausnahme ist iZm sozialen Netzwerken „*spannend*".

[535] *Höch/Kahl*, Anforderungen an eine Kennzeichnungspflicht für KI-Inhalte, KuR 2023, 396 (396).

hochwertige und informative Inhalte zu produzieren und somit ihre journalistische Sorgfalt zu bewahren.[536]

Deepfakes spielen natürlich auch eine unverkennbare Rolle iZm politischer Werbung,[537] sodass KI-Systeme, die verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts in einer Wahl oder in Referenden zu beeinflussen, jedenfalls als Hochrisiko-KI-Systeme eingestuft werden (Art 6 Abs 2 KI-VO iVm Anhang III Z 8 lit b KI-VO, ErwGr 62 KI-VO).

3.6.4 Abgrenzung zu Transparenzpflichten für Hochrisiko-KI

Art 50 Abs 6 KI-VO normiert, dass die Kennzeichnungspflichten gem Art 50 Abs 1-4 KI-VO *„die in Kapitel III festgelegten Anforderungen und Pflichten unberührt [lassen]*“,[538] um Bedenken hinsichtlich der Undurchsichtigkeit und Komplexität dieser KI-Systeme auszuräumen und die Betreiber bei der Erfüllung ihrer Pflichten gem der KI-VO zu unterstützen (ErwGr 72 KI-VO). Somit gilt es bei hochriskanten KI-Systemen parallel die besonderen Transparenzpflichten nach Art 12 ff KI-VO zu beachten, bevor sie in Verkehr gebracht oder in Betrieb genommen werden.[539] Schon die Technik der Hochrisiko-KI-Systeme[540] muss die automatische Aufzeichnung von Ereignissen während des Lebenszyklus des Systems ermöglichen (Art 12 KI-VO: *„Aufzeichnungs- bzw Protokollierungspflicht*“).[541] Wichtig sind zudem die Verpflichtungen zur

[536] *Leitl-Staudinger* in *Mayrhofer/Nessler/Bieber/Fister/Homar/Tumpel* (Hrsg), ChatGPT, Gemini & Co (2024) 112.

[537] Vgl VO (EU) 2024/900, ABl 2024/Reihe L, 1: Diese neue VO über die Transparenz und das Targeting politischer Werbung wurde entwickelt, um Bedenken hinsichtlich der Gefahren zu adressieren, die von manipulierten Informationen und der Beeinflussung von Wahlen aus dem Ausland ausgehen. Sie soll es den Bürgerinnen und Bürgern erleichtern, politische Anzeigen als solche zu erkennen, zu verstehen, wer dahintersteckt, und festzustellen, ob es sich um personalisierte politische Anzeigen handelt. Dadurch sollen sie besser in der Lage sein, fundierte Entscheidungen zu treffen; vgl Rat 11.3.2024, EU führt neue Vorschriften über Transparenz und Targeting politischer Werbung ein, abrufbar unter <https://www.consilium.europa.eu/de/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising> (5.5. 2024).

[538] Die Einhaltung der Transparenzpflichten für die von der KI-VO erfassten KI Systeme sollte nicht als Hinweis dafür ausgelegt werden, dass die Verwendung des Systems oder seines Ergebnisses nach der KI-VO oder anderen Rechtsvorschriften der EU und der MS rechtmäßig ist (ErwGr 137 KI-VO).

[539] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 134: Insb richten sich Art 50 KI-VO und Art 13 KI-VO an einen unterschiedlichen Adressatenkreis.

[540] Vgl die „*Technische Dokumentation*“ (Art 11 KI-VO iVm Anhang IV KI-VO): Diese Informationen sollten ua die allgemeinen Merkmale, Fähigkeiten und Grenzen des Systems, die verwendeten Algorithmen, Daten und Trainings-, Test- und Validierungsverfahren enthalten (ErwGr 71 KI-VO).

[541] *Spindler*, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E), CR 2021, 361 (367); *Hoffmann*, Regulierung der Künstlichen Intelligenz, KuR 2021, 369 (372).

funktionalen Transparenz und Bereitstellung von Informationen in Form von Betriebsanleitungen (Art 13 KI-VO) sowie die Sicherstellung einer menschlichen Aufsicht (Art 14 KI-VO).[542]

Hochrisiko-KI-Systeme müssen zunächst so konzipiert und entwickelt werden, dass ihr Betrieb hinreichend transparent ist („*funktionale Transparenz*“: Art 13 Abs 1 KI-VO).[543] Diese Transparenz muss auf eine geeignete Art und in einem angemessenen Maß gewährleistet werden, damit die Anbieter und Betreiber ihre einschlägigen Pflichten gem Art 16 ff KI-VO erfüllen können. Hauptsächlich sollen dadurch die Betreiber in die Lage versetzt werden, die Ergebnisse des Systems angemessen zu interpretieren und zu nutzen. Sie sollen verstehen können, wie das KI-System funktioniert, seine Funktionalität bewerten und sowohl seine Stärken als auch seine Grenzen erfassen können (ErwGr 72 KI-VO). Funktionale Transparenz dient somit einerseits der Gewährleistung der tatsächlichen Nutzbarkeit des KI-Systems und andererseits einem Beitrag zur Einhaltung der Vorschriften der KI-VO.[544] Die konkret „*geeignete und angemessene*“ Ausgestaltung dieser Transparenzpflicht bleibt aber den Anbietern überlassen.[545] Die KI-VO verlangt bloß, dass „*in der gesamten Dokumentation [...] aussagekräftige, umfassende, zugängliche und verständliche Informationen enthalten sind, wobei die Bedürfnisse und vorhersehbaren Kenntnisse der Zielbetreiber zu berücksichtigen sind*“ (ErwGr 72 vorletzter Satz KI-VO). Eine „*vollständige Systemtransparenz*“ [546] iSe Offenlegungspflicht, wie der Algorithmus zu seiner Entscheidungsfindung gelangt, lässt sich daraus – ein weiteres Mal – nicht ableiten.

Abhilfe könnte mE die in Art 13 Abs 2 KI-VO festgelegte Pflicht zur Bereitstellung einer Betriebsanleitung[547] bieten. In dieser sollten alle bekannten oder vorhersehbaren Umstände iZm der ordnungsgemäßen Verwendung eines Hochrisiko-KI-Systems oder einer vernünftigerweise vorhersehbaren Fehlanwendung aufgeführt werden, die zu Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können (ErwGr 65 KI-VO). Die Betreiber sollten

[542] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 12.
[543] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 16.
[544] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 17.
[545] *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, 528 (534).
[546] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 20.
[547] Das sind die Informationen, die der Anbieter bereitstellt, um den Betreiber insb über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI Systems zu informieren (Art 3 Z 15 KI-VO). Diese müssen in einem geeigneten digitalen Format oder auf andere Weise präzise, vollständig, korrekt und eindeutig bereitgestellt werden. Außerdem müssen sie in einer für die Betreiber relevanten, barrierefrei zugänglichen und verständlichen Form vorliegen (Art 13 Abs 2 KI-VO).

diese Umstände bei der Nutzung kennen und berücksichtigen können.[548] Genauer gesagt muss die Betriebsanleitung Mindestinformationen enthalten (Art 13 Abs 3 KI-VO), welche ua Angaben zu den Merkmalen, (technischen) Fähigkeiten und Leistungsgrenzen des Hochrisiko-KI-Systems inkludieren (vgl auch ErwGr 72 KI-VO). Zu diesen zählen bspw (i) Informationen, die „*zur Erläuterung seiner Ergebnisse relevant sind*", (ii) Informationen über „*seine Leistung in Bezug auf bestimmte Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll*", (iii) Informationen, „*die es den Betreibern ermöglichen, das Ergebnis des Hochrisiko-KI-Systems zu interpretieren und es angemessen zu nutzen*", sowie (iv) eine „*Beschreibung der [...] integrierten Mechanismen*". Ob dies letztendlich zu einer tatsächlichen Offenlegung des „*Ob*" und „*Wie*" einer Entscheidungsfindung führt, kann – insb im Hinblick auf die Wahrung von Betriebs- und Geschäftsgeheimnissen – angezweifelt werden und erfordert meiner Meinung nach eine abschließende Klärung durch die EK.

Um den Anforderungen an eine auf den Menschen ausgerichtete KI gerecht zu werden und das Vertrauen in KI zu stärken,[549] sieht Art 14 KI-VO die sog „*menschliche Aufsicht*" vor.[550] Der Mensch sollte in der Lage sein, potenzielle Risiken für grundlegende Rechtspositionen zu verhindern oder minimieren (Art 14 Abs 2 KI-VO).[551] Hierfür braucht es bereits vor dem Inverkehrbringen oder der Inbetriebnahme geeignete TOM (ErwGr 73, 91 KI-VO). Das System muss an erster Stelle integrierten Betriebseinschränkungen unterliegen, über die sich das Hochrisiko-KI-System – zB bei Bonitätsprüfungen für Kredite[552] – selbst nicht hinwegsetzen kann. Ferner muss es auf den menschlichen Bediener reagieren und gewährleisten können, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, um diese Aufgabe wahrzunehmen (vgl Art 4 KI-VO bzgl der „*KI-Kompetenz*").[553] Des Weiteren müssen Mechanismen enthalten sein, um eine natürliche Person, der die menschliche Aufsicht übertragen wurde, zu beraten und zu informieren, damit diese fundierte Entscheidungen darüber treffen kann, (i) ob, wann und wie

[548] Insb iZm ihrer Pflicht zur Erstellung einer DSFA (Art 26 Abs 9 KI-VO iVm Art 35 DSGVO).

[549] *Kalbhenn*, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme, ZUM 2021, 663 (668).

[550] „*Menschliches Handeln und menschliche Aufsicht*" bedeutet, dass ein KI-System entwickelt und als Instrument verwendet wird, das den Menschen dient, die Menschenwürde und die persönliche Autonomie achtet und so funktioniert, dass es von Menschen angemessen kontrolliert und überwacht werden kann (ErwGr 27 KI-VO).

[551] *Linardatos*, Auf dem Weg zu einer europäischen KI-Verordnung, GPR 2022, 58 (58 ff).

[552] *Zankl*, KI: Hohes Risiko nur unter menschlicher Aufsicht, Die Presse - Recht 2021/147.

[553] *Becker/Feuerstack*, Der neue Entwurf des EU-Parlaments für eine KI-Verordnung, MMR 2024, 22 (24 f).

einzugreifen ist, um negative Folgen oder Risiken zu vermeiden, oder (ii) das KI-System (notfalls) anzuhalten, wenn es nicht wie beabsichtigt funktioniert.

Angesichts dieser Überlegungen müssen Hochrisiko-KI-Systeme vom Anbieter so gestaltet und entwickelt werden (vgl Art 14 Abs 3 KI-VO), dass sie während ihrer Verwendungsdauer von natürlichen Personen wirksam überwacht werden können (Art 14 Abs 1 KI-VO).[554] Die menschlichen Aufsichtspersonen (auf Seiten des Betreibers) müssen gem Art 14 Abs 4 KI-VO angemessen und verhältnismäßig in der Lage sein: (a) die relevanten Fähigkeiten und Grenzen dieses KI-Systems angemessen zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, einschließlich der Erkennung und Behebung von Anomalien, Fehlfunktionen und unerwarteter Leistungen, (b) sich der potenziellen Neigung zu einem automatischen oder übermäßigen Vertrauen in den Output eines Hochrisiko-KI-Systems („*Automatisierungsbias*“)[555] bewusst zu sein, insb wenn es Informationen oder Empfehlungen bereitstellt, auf deren Grundlage natürliche Personen Entscheidungen treffen, (c) den Output des Hochrisiko-KI-Systems richtig zu interpretieren (d) in bestimmten Situationen doch zu entscheiden, das Hochrisiko-KI-System nicht zu verwenden oder seinen Output zu ignorieren, aufzuheben oder rückgängig zu machen („*Panic Button*“),[556] und (e) in den Betrieb des Hochrisiko-KI-Systems einzugreifen oder den Systembetrieb mit einer „*Stopptaste*“ oder einem ähnlichen Verfahren zu unterbrechen, um das System sicher zum Stillstand zu bringen.

Bei biometrischen Fernidentifizierungssystemen gelten strengere Anforderungen an die menschliche Aufsicht (Art 14 Abs 5 KI-VO): Der Betreiber darf keine Maßnahmen oder Entscheidungen nur aufgrund des erzeugten Identifizierungsergebnisses treffen, solange die Identifizierung nicht von mind zwei natürlichen Personen separat überprüft und bestätigt wurde. Diese Personen können von einer oder mehreren Einrichtungen stammen und die Person umfassen, die das System bedient oder verwendet (ErwGr 73 KI-VO).

[554] Etwa durch geeignete „*Mensch-Maschine-Schnittstellen*“ (human-machine interface tools); vgl *Frank/Heine*, KI-Einsatz im Betrieb unter der KI-Verordnung, NZA 2023, 1281 (1283).

[555] *Alon-Barkat/Busuioc*, Human–AI Interactions in Public Sector Decision Making: “Automation Bias” and “Selective Adherence” to Algorithmic Advice, Journal of Public Administration Research and Theory 2023, 153 (154).

[556] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 27.

Der Vollständigkeit halber wird auf die sog „*EU-Datenbank für Hochrisiko-KI-Systeme*“ hingewiesen (Art 71 KI-VO iVm ErwGr 131 KI-VO). Diese ermöglicht der Öffentlichkeit[557] ua auch die Einsicht in die Zweckbestimmung des KI-Systems, in grundlegende und knappe Beschreibungen der vom System verwendeten Informationen (Daten, Eingaben) und seiner Betriebslogik sowie in die elektronischen Betriebsanleitungen (vgl Anhang VIII Abschnitt A).

3.7 Daten-Governance

3.7.1 Training von Hochrisiko-KI

Eine iZm dem Datenschutz und dem Training von KI wesentliche Bestimmung ist Art 10 KI-VO.[558] Dieser regelt, dass Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, mit qualitativen Trainings-, Validierungs- und Testdatensätzen[559] entwickelt werden müssen, wenn solche Datensätze (überhaupt) verwendet werden (Art 10 Abs 1 KI-VO).

Derartige Trainings-, Validierungs- und Testdatensätze sollen Daten-Governance- und Datenverwaltungsverfahren unterliegen, die für den vorgesehenen Zweck des Hochrisiko-KI-Systems geeignet sind (Art 10 Abs 2 KI-VO). Diese Verfahren betreffen ua auch die Datenerhebungsverfahren, die Herkunft der Daten und – im Falle personenbezogener Daten – den ursprünglichen Zweck der Datenerhebung[560] sowie Datenaufbereitungsvorgänge wie etwa die Annotation, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregierung. Des Weiteren beziehen sich die Verfahren auf die Aufstellung von Annahmen (insb in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen) und die

[557] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 31.

[558] „*Privatsphäre und Daten-Governance*“ bedeutet, dass KI-Systeme im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz entwickelt und verwendet werden und dabei Daten verarbeiten, die hohen Qualitäts- und Integritätsstandards genügen (ErwGr 27 KI-VO).

[559] „*Trainingsdaten*“ sind Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden (Art 3 Z 29 KI-VO). „*Validierungsdaten*“ sind Daten, die zur Evaluation des trainierten KI-Systems und zur Einstellung seiner nicht erlernbaren Parameter und seines Lernprozesses verwendet werden, um ua eine Unter- oder Überanpassung zu vermeiden (Art 3 Z 30 KI-VO). Ein „*Validierungsdatensatz*“ ist dabei ein separater Datensatz oder ein Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung (Art 3 Z 31 KI-VO). „*Testdaten*“ sind Daten, die für eine unabhängige Bewertung des KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen (Art 3 Z 32 KI-VO).

[560] Um die Einhaltung des Datenschutzrechts der Union, wie der DSGVO, zu erleichtern (ErwGr 67 KI-VO).

Bewertung der Verfügbarkeit, Menge[561] und Eignung der benötigten Datensätze. Die Verfahren müssen auch Untersuchungen im Hinblick auf mögliche Verzerrungen („*Bias*“)[562] beinhalten,[563] die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach Unionsrecht verbotenen Diskriminierung führen könnten[564] (insb wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen: sog „*Rückkopplungsschleifen*“ bzw „*Feedback Loops*“).[565] Daher sind geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher Verzerrungen erforderlich.

Bemerkenswert ist, dass diesbezüglich eine partielle Durchbrechung[566] von Art 9 DSGVO vorgesehen ist (Art 10 Abs 5 KI-VO): Nur soweit dies „*für die Erkennung und Korrektur von Verzerrungen[567] iZm Hochrisiko-KI-Systemen unbedingt erforderlich*“ ist, dürfen die Anbieter – und nicht zB auch die Betreiber[568] – solcher Systeme ausnahmsweise[569] besondere Kategorien personenbezogener Daten verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen.

---

[561] *Spindler* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 5 Rz 23: Hinsichtlich der Menge sollte es sich um eine ausreichende statistische Basis handeln, da ein Training nur auf der Grundlage weniger Daten kaum sinnvoll erscheint. Aus datenschutzrechtlicher Perspektive ist dies mE – falls und soweit es personenbezogene Daten betrifft – zu hinterfragen, da dies evtl im Konflikt mit den bereits aufgezeigten Grenzen der Verarbeitungsgrundsätze gem Art 5 DSGVO steht, insb dem Grundsatz der Datenminimierung. Auch ErwGr 69 KI-VO geht davon aus, dass Datenminimierung, Privacy by Default sowie Privacy by Design bei der Verarbeitung personenbezogener Daten beachtet werden müssen.

[562] „*Vielfalt, Nichtdiskriminierung und Fairness*“ bedeutet, dass KI-Systeme in einer Weise entwickelt und verwendet werden, die unterschiedliche Akteure einbezieht und den gleichberechtigten Zugang, die Geschlechtergleichstellung und die kulturelle Vielfalt fördert, wobei diskriminierende Auswirkungen und unfaire Verzerrungen, die nach EU-Recht oder nationalem Recht verboten sind, verhindert werden (ErwGr 27 KI-VO). Verzerrungen können – insb bei Verwendung historischer Daten – den zugrunde liegenden Datensätzen innewohnen oder bei der Implementierung der Systeme in der realen Welt generiert werden (ErwGr 67 KI-VO).

[563] Vgl *Pek* in *Chibanguza/Kuß/Steege* (Hrsg), Künstliche Intelligenz (2022) § 6 B Rz 4 ff.

[564] Die von einem KI-System generierten Ergebnisse könnten durch solche inhärenten Verzerrungen beeinflusst werden, die tendenziell zunehmen und bestehende Diskriminierungen, insb gegenüber Personen, die bestimmten schutzbedürftigen Gruppen – wie zB rassistisch benachteiligten oder ethnischen Gruppen – angehören, fortsetzen und verstärken (ErwGr 67 KI-VO).

[565] Diese gewährleisten, dass KI-Testsysteme nicht nur vorprogrammierte Anweisungen befolgen, sondern aktiv aus ihren Handlungen lernen. Sie bewerten und verbessern kontinuierlich die Testmöglichkeiten basierend auf den Erkenntnissen jedes Testdurchlaufs. Die Wirksamkeit von Feedbackschleifen variiert je nach Art des Lernsystems und sorgt dafür, dass das System mit jeder Testdurchführung intelligenter, produktiver und verlässlicher wird; vgl *Lenz* in *Harwardt/Niermann/Schmutte/Steuernagel* (Hrsg), Lernen im Zeitalter der Digitalisierung (2023) 161 ff.

[566] *Spindler* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 5 Rz 21.

[567] *Spindler* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 5 Rz 32: Nicht für das „*normale*“ Testen oder Trainieren.

[568] *Spindler* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 5 Rz 34: Für Betreiber bleibt es also bei einem Verbot der Verarbeitung sensibler Daten, es sei denn, es liegt eine Ausnahme gem Art 9 Abs 2 DSGVO (insb eine explizite Einwilligung) vor.

[569] Dh als Angelegenheit von erheblichem öffentlichen Interesse iSd Art 9 Abs 2 lit g DSGVO (ErwGr 70 KI-VO).

Zusätzlich zu den Bestimmungen der DSGVO müssen dafür alle folgenden Bedingungen erfüllt sein: (a) Die Erkennung und Korrektur von Verzerrungen kann durch die Verarbeitung anderer Daten, inkl synthetischer oder anonymisierter Daten, nicht effektiv durchgeführt werden, (b) die sensiblen Daten unterliegen technischen Beschränkungen einer Weiterverwendung der personenbezogenen Daten und modernsten Sicherheits- und Datenschutzmaßnahmen, einschließlich Pseudonymisierung, (c) die besonderen Kategorien personenbezogener Daten unterliegen Maßnahmen, mit denen sichergestellt wird, dass die verarbeiteten personenbezogenen Daten gesichert, geschützt und Gegenstand angemessener Sicherheitsvorkehrungen sind, wozu auch strenge Kontrollen des Zugriffs und seine Dokumentation gehören, um Missbrauch zu verhindern und sicherzustellen, dass nur befugte Personen Zugang zu diesen personenbezogenen Daten mit angemessenen Vertraulichkeitspflichten haben, (d) die sensiblen Daten werden weder an Dritte übermittelt oder übertragen noch haben diese Dritten anderweitigen Zugang zu diesen Daten, (e) die sensiblen Daten werden gelöscht, sobald die Verzerrung korrigiert wurde oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist, je nachdem, was zuerst eintritt,[570] und (f) das VVT (Art 30 DSGVO) enthält die Gründe, warum die Verarbeitung besonderer Kategorien personenbezogener Daten für die Erkennung und Korrektur von Verzerrungen unbedingt erforderlich war und warum dieses Ziel mit der Verarbeitung anderer Daten nicht erreicht werden konnte.

Zur geforderten Qualität[571] der Trainings-, Validierungs- und Testdatensätze bestimmt Art 10 Abs 3 KI-VO folgendes: Auf der einen Seite müssen sie – inkl der Kennzeichnungen (ErwGr 67 KI-VO) – im Hinblick auf die Zweckbestimmung „*relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig*“[572] sein. Auf der anderen Seite müssen sie die „*geeigneten statistischen Merkmale*“,[573] evtl auch bzgl der Personen oder Personengruppen, für

[570] Dass die Erkenntnisse beim Anbieter verbleiben und evtl für weitere Anwendungen genutzt werden könnten, ist somit zu relativieren; vgl *Ebert/Spiecker*, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188 (1190).

[571] Die Bereitstellung hochwertiger Daten und der Zugang dazu sind von zentraler Bedeutung für die Leistung vieler KI-Systeme. Dadurch wird sichergestellt, dass das Hochrisiko-KI-System ordnungsgemäß und sicher funktioniert und nicht zur Ursache für Diskriminierung wird (ErwGr 67 KI-VO).

[572] Es fällt auf, dass keine vollständige Fehlerfreiheit gefordert wird, da es äußerst unwahrscheinlich ist, dass die für das Training von (Hochrisiko-)KI-Systemen verwendeten Daten gänzlich frei von Fehlern sind. Darüber hinaus kann das Training grds auch auf unvollständigen Datensätzen basieren; vgl *Spindler* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 5 Rz 26.

[573] Insb müssen die Datensätze, soweit dies für die Zweckbestimmung erforderlich ist, den Eigenschaften, Merkmalen oder Elementen entsprechen, welche für die besonderen geografischen, kontextuellen,

die das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll,[574] haben.[575] Diese Merkmale können auf der Ebene von Einzeldatensätzen oder (erst) durch die Kombination mehrerer solcher Datensätze erreicht werden.[576] Die Rechtsanwendungspraxis wird sich ua aber die Frage stellen müssen, ob und in welchem Ausmaß ein Verstoß gegen die DSGVO während der Trainingsphase zu einer Fehlerhaftigkeit iSd KI-VO führt.[577]

3.7.2 Training von GPAI

Alle Anbieter[578] von GPAI[579] unterliegen speziellen Transparenzpflichten gem Art 53 KI-VO.[580]

Dazu gehört die Verpflichtung, eine „*technische Dokumentation*" (Art 53 Abs 1 lit a KI-VO iVm Anhang XI Abschnitt 1 KI-VO) zu erstellen.[581] Diese muss nicht nur eine allgemeine Beschreibung[582] des KI-Modells enthalten, sondern auch detaillierte und aktuelle Informationen zu seinen Elementen (vgl ErwGr 101 KI-VO).

---

verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind (Art 10 Abs 4 KI-VO).

574 *Müller-Peltzer/Tanczik*, Künstliche Intelligenz und Daten, RDi 2023, 452 (455): Es scheint so zu sein, dass die KI-Anbieter selbst entscheiden können und müssen, ob es sich bei den vom KI-System potenziell betroffenen Personen um eine repräsentative Stichprobe der Gesamtbevölkerung oder nur um eine spezifische Gruppe handelt, auf die das System angewandt wird oder für die es entsprechende Ergebnisse liefert.

575 *Hacker*, A legal framework for AI training data – from first principles to the Artificial Intelligence Act, Law, Innovation and Technology 2021, 257 (297): Die KI-VO deckt im Vergleich zu dem in Art 5 Abs 1 lit d DSGVO verankerten Grundsatz der Datenqualität („*sachlich richtig und erforderlichenfalls auf dem neuesten Stand*") wesentlich mehr Kriterien ab.

576 In diesem Zusammenhang ist mE problematisch, dass allein die Überprüfung der Datensätze auf die genannten Qualitätskriterien eine Verarbeitung personenbezogener Daten iSd der DSGVO darstellen könnte. Anbieter benötigen also aller Voraussicht nach eine Rechtsgrundlage (Einwilligung) iSd Art 6 bzw Art 9 DSGVO.

577 *Paal*, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, ZfDR 2024, 129 (155).

578 *Lachenmann*, EU-Rat stimmt KI-Verordnung zu – neue Pflichten für Unternehmen, MMR-Aktuell 2024, 01359 (beck-online): Betreiber treffen keine zusätzlichen Pflichten.

579 Diese sind gekennzeichnet durch ihre allgemeine Verwendbarkeit und der Fähigkeit, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen. Sie werden idR mit großen Datenmengen durch verschiedene Methoden, etwa überwachtes, unüberwachtes und bestärkendes Lernen, trainiert (ErwGr 97 ff KI-VO).

580 Zusätzlich zu diesen Vorschriften gelten für alle Anbieter von GPAI die spezifischen Transparenz- und Kennzeichnungspflichten gem Art 50 KI-VO. Anbieter von GPAI mit systemischem Risiko (Art 51 KI-VO iVm Anhang XIII KI-VO, ErwGr 111 ff KI-VO) haben darüber hinaus weitergehende Pflichten gem Art 55 KI-VO iVm Anhang XI Abschnitt 2 KI-VO; vgl *Anderl/Ciarnau*, Sprach-KI als „systemisches Risiko", Der Standard 2023/2381380.

581 Sofern es sich nicht um einen Anbieter einer GPAI handelt, die im Rahmen einer freien und quelloffenen Lizenz („*free and open source*") bereitgestellt wird und kein systemisches Risiko aufweist (Art 53 Abs 2 KI-VO). Deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung müssen öffentlich zugänglich gemacht werden (vgl ErwGr 102 ff KI-VO).

582 Konkret die Aufgaben, die das Modell erfüllen soll, die Art und das Wesen der KI-Systeme, in die es integriert werden kann, die anwendbaren Regelungen der akzeptablen Nutzung, das Datum der Freigabe und die Vertriebsmethoden, die Architektur und die Anzahl der Parameter, die Modalität (zB Text, Bild) und das Format der Ein- und Ausgaben.

Diese umfassen wesentliche Angaben zum Entwicklungs- und Trainingsverfahren, einschließlich der verwendeten Trainingsmethoden und -techniken. Des Weiteren müssen Informationen darüber bereitgestellt werden, was das Modell optimieren soll und welche Rolle den verschiedenen Parametern dabei zukommt. Auch Angaben über die für das Training, Testen und Validieren verwendeten Daten, einschließlich ihrer Art, Herkunft, Aufbereitungsmethoden, Umfang und Hauptmerkmale, sind erforderlich.[583] Schließlich müssen auch die Methoden zur Datenerfassung und Auswahl – also die Art und Weise, wie die Daten erlangt und ausgewählt wurden – sowie „*andere relevante Einzelheiten iZm dem Trainieren*" offengelegt werden. Solch eine detaillierte Transparenz muss jedoch nur auf Anfrage dem KI-Büro (Art 64 KI-VO) und den zuständigen nationalen Behörden (Art 70 KI-VO) zur Verfügung gestellt werden.

Gegenüber der Allgemeinheit besteht dagegen (nur) die Pflicht zur Erstellung und Veröffentlichung einer „*hinreichend detaillierten*" Zusammenfassung der für das Training der GPAI verwendeten Inhalte nach einer vom KI-Büro bereitgestellten Vorlage (Art 53 Abs 1 lit d KI-VO).

Möchten Anbieter von KI-Systemen eine GPAI in ihr KI-System integrieren, müssen die GPAI-Anbieter[584] diesen ihre Dokumentation – mit einem bestimmten Mindestinhalt (vgl Anhang XII KI-VO) – zur Verfügung stellen, damit diese „*nachgelagerten*" Anbieter von KI-Systemen die Fähigkeiten und Grenzen der GPAI gut verstehen können (Art 53 Abs 1 lit b KI-VO).

Hingewiesen wird auf die – mE begrüßenswerte – Pflicht zur Erstellung einer „*Strategie zur Einhaltung des Urheberrechts*" (Art 53 Abs 1 lit c KI-VO),[585] auf die nicht näher eingegangen wird.

[583] *Dieker*, Datenschutzrechtliche Zulässigkeit der Trainingsdatensammlung, ZD 2024, 132 (132 ff): Ausführlich zu datenschutzrechtlichen Anmerkungen – insb zum berechtigten Interesse – hinsichtlich der Frage, wie Scraping und Crawling zur KI-Entwicklung eingesetzt werden können.

[584] Außer Anbieter einer GPAI, die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt wird und kein systemisches Risiko aufweist (Art 53 Abs 2 KI-VO).

[585] Vgl hierzu insb ErwGr 104 ff KI-VO und § 42h Abs 6 UrhG, BGBl Nr 111/1936 idF BGBl I Nr 182/2023: Zum Nutzungsvorbehalt bzgl Text- und Data-Mining.

3.7.3 KI-Reallabore & Datenschutz

Ein „*KI-Reallabor*“ („*Regulatory Sandbox*“)[586] bietet eine überwachte Umgebung, um Innovationen voranzutreiben und die Entwicklung, das Training und Testen sowie die Validierung moderner KI-Systeme vor ihrem tatsächlichen Einsatz zu erleichtern (Art 57 Abs 5 KI-VO iVm ErwGr 138 ff KI-VO).[587] In diesen können auch beaufsichtigte „*Tests unter Realbedingungen*“[588] durchgeführt werden. Nichtsdestotrotz sollen in den Reallaboren auch Risiken der KI-Systeme – insb im Hinblick auf potenzielle Grundrechtseingriffe – aufgedeckt werden (Art 57 Abs 6 KI-VO). Es ist mE daher sehr erfreulich, dass die nationalen DSB in den Betrieb eines KI-Reallabors und in die Überwachung dieser Aspekte vollständig einbezogen werden müssen, soweit die zu entwickelnden, zu testenden oder zu trainierenden KI-Systeme Daten mit Personenbezug verarbeiten (Art 57 Abs 10 KI-VO).

Hingegen normiert die KI-VO eine zweite[589] gravierende Durchbrechung der DSGVO, da die „*Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im erheblichen öffentlichen Interesse*“ ermöglicht wird (Art 59 KI-VO). Dadurch kommt es zu einer

[586] Das ist ein kontrollierter Rahmen, der von einer zuständigen (nationalen) Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter Realbedingungen – zu testen (Art 3 Z 55 KI-VO).

[587] *Voß* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 9 Rz 1 ff.

[588] Das ist ein befristeter Test eines KI-Systems auf seine Zweckbestimmung, der unter Realbedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung erfolgt, um zuverlässige und belastbare Daten zu erheben und die Konformität des KI-Systems mit den Anforderungen der KI-VO zu bewerten und zu überprüfen, wobei dieser Test nicht als Inverkehrbringen oder Inbetriebnahme des KI-Systems gilt (Art 3 Z 57 KI-VO). Außerhalb von KI-Reallaboren (vgl Art 60 KI-VO) erfordert die Teilnahme an solchen Tests unter Realbedingungen die „*informierte Einwilligung*“ der Testteilnehmer (Art 61 KI-VO). Das ist eine aus freien Stücken erfolgende, spezifische, eindeutige und freiwillige Erklärung der Bereitschaft, an einem bestimmten Test unter Realbedingungen teilzunehmen, durch einen Testteilnehmer (vgl Art 3 Z 58 KI-VO), nachdem dieser über alle Aspekte des Tests, die für die Entscheidungsfindung des Testteilnehmers bzgl der Teilnahme relevant sind, aufgeklärt wurde (Art 3 Z 59 KI-VO). Diese (widerrufliche) Einwilligung der Testteilnehmer zur Teilnahme an solchen Tests unterscheidet sich von der Einwilligung betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten nach den einschlägigen Datenschutzvorschriften und greift dieser nicht vor (ErwGr 141 KI-VO). Es sollte erwähnt werden, dass die KI-VO nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen gilt, bevor diese in Verkehr gebracht oder in Betrieb genommen werden (Art 2 Abs 8 KI-VO). Solche Tätigkeiten müssen aber im Einklang mit dem geltenden EU-Recht durchgeführt. Tests unter Realbedingungen und die Anwendung der Bestimmungen zu KI-Reallaboren fallen ohnehin nicht unter diesen Ausschluss (ErwGr 25 KI-VO).

[589] Vgl Kapitel 3.7.1 (Training von Hochrisiko-KI): Art 10 Abs 5 KI-VO.

Abkehr vom Zweckbindungsgrundsatz (Art 5 Abs 1 lit b DSGVO) sowie zu einer Ergänzung[590] von Art 6 Abs 4 DSGVO.[591]

Dessen ungeachtet hängt die mögliche Berufung auf diesen „*Erlaubnistatbestand*"[592] bzw diese (zusätzliche) „*Rechtsgrundlage*"[593] von der Einhaltung äußerst strenger Voraussetzungen ab. Konkret müssen alle der folgenden Bedingungen erfüllt sein: (i) personenbezogene Daten müssen rechtmäßig[594] für die Weiterverarbeitung für andere Zwecke erhoben worden sein, (ii) das KI-System wird im Reallabor zur Wahrung eines taxativ aufgezählten, erheblichen öffentlichen Interesses[595] – also gerade nicht für Zwecke der (personalisierten) Werbung – entwickelt, (iii) die verarbeiteten Daten sind für die Erfüllung einer oder mehrerer der in Art 8 ff KI-VO genannten Anforderungen[596] erforderlich, sofern diese nicht durch die Verarbeitung anonymisierter, synthetischer oder sonstiger nicht-personenbezogener Daten wirksam erfüllt werden können, (iv) es bestehen wirksame Überwachungsmechanismen – iSe DSFA –, mit deren Hilfe festgestellt wird, ob während der Reallaborversuche hohe Risiken für die Rechte und Freiheiten Betroffener auftreten können, sowie Reaktionsmechanismen, mit deren Hilfe diese Risiken umgehend eingedämmt werden können und die Verarbeitung bei Bedarf beendet werden kann, (v) die personenbezogene Daten müssen sich in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle des zukünftigen Anbieters befinden, wobei nur befugte Personen Zugriff auf diese Daten haben dürfen, (vi) Anbieter dürfen die ursprünglich erhobenen Daten nur im Einklang mit EU-Datenschutzrecht weitergeben; personenbezogene Daten, die im Reallabor erstellt wurden, dürfen nicht

590 *Voß* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 9 Rz 28.

591 Vgl Kapitel 2.3.1 (Nutzung privater ChatGPT-Accounts).

592 *Bomhard/Merkle*, Europäische KI-Verordnung, RDi 2021, 276 (279).

593 Die KI-VO sollte „*im Einklang mit*" Art 6 Abs 4 DSGVO und Art 9 Abs 2 lit g DSGVO die „*Rechtsgrundlage*" für die Verwendung – ausschließlich unter bestimmten Bedingungen – personenbezogener Daten, die für andere Zwecke erhoben wurden, zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse innerhalb des KI-Reallabors durch die Anbieter und zukünftigen Anbieter im KI-Reallabor bilden (ErwGr 140 KI-VO). Das ist nunmehr konform mit ErwGr 63 KI-VO; vgl auch EDSA/EDSB 18.6.2021, Gemeinsame Stellungnahme 5/2021, Rz 64.

594 *Voß* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 9 Rz 29: Dies setzt idR die Einwilligung der Betroffenen voraus.

595 Zu diesen gehören die öffentliche Sicherheit, öffentliche Gesundheit, der Umwelt- und Klimaschutz, nachhaltige Energie, Sicherheit und Widerstandsfähigkeit von Verkehrssystemen und Mobilität, kritischen Infrastrukturen und Netzen sowie letztlich die Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste.

596 Risikomanagement (Art 9 KI-VO), Daten-Governance (Art 10 KI-VO), Technische Dokumentation (Art 11 KI-VO), Aufzeichnung (Art 12 KI-VO), Transparenz (Art 13 KI-VO), Menschliche Aufsicht (Art 14 KI-VO) und/oder Genauigkeit, Robustheit und Cybersicherheit (Art 15 KI-VO).

außerhalb des Reallabors weitergegeben werden, (vii) eine Verarbeitung personenbezogener Daten führt zu keinen Maßnahmen oder Entscheidungen, die Auswirkungen auf die Betroffenen haben, und berührt nicht die Anwendung ihrer Rechte, die in den Rechtsvorschriften der Union über den Schutz personenbezogener Daten festgelegt sind,[597] (viii) verarbeitete personenbezogene Daten müssen durch geeignete TOM geschützt werden und werden gelöscht, sobald die Beteiligung an dem Reallabor endet oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist,[598] (ix) eine vollständige und detaillierte Beschreibung des Prozesses und der Gründe für das Trainieren, Testen und Validieren des KI-Systems wird zusammen mit den Testergebnissen als Teil der technischen Dokumentation aufbewahrt, sowie (x) es muss eine kurze Zusammenfassung des im Reallabor entwickelten KI-Projekts, seiner Ziele und der erwarteten Ergebnisse auf der Website der zuständigen Behörden veröffentlicht werden.

Für KI-Betreiber möglicherweise interessant ist die Möglichkeit, gemeinsam mit dem Anbieter einen Antrag auf Zugang und Beteiligung an einem KI-Reallabor zu stellen (Art 58 Abs 2 KI-VO). Zusätzlich könnten die nach Anhang III gelisteten Hochrisiko-KI-Systeme zusammen mit den Anbietern auch außerhalb eines KI-Reallabors unter Realbedingungen getestet werden, wobei auf die Einholung einer speziellen Einwilligung (Art 61 KI-VO) der Testteilnehmer zu achten ist (Art 60 Abs 2 KI-VO) und ein Vertrag mit dem Anbieter abgeschlossen werden müsste (Art 60 Abs 4 lit h KI-VO).

3.8 Verhältnis zwischen KI-VO & DSGVO

3.8.1 Gemeinsamkeiten

Wie die DSGVO beruht die KI-VO auf Art 16 AEUV. Dieser normiert einerseits das Grundrecht auf Datenschutz (Art 16 Abs 1 AEUV)[599] und sieht andererseits eine geteilte Zuständigkeit

[597] Alle Pflichten von Verantwortlichen und die Rechte der Betroffenen gem der DSGVO gelten weiterhin (ErwGr 140 KI-VO).

[598] *Ebert/Spiecker*, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188 (1192): Angesichts der Tatsache, dass personenbezogene Daten oft auch nachträglich aus trainierten KI-Systemen rekonstruiert werden können, erscheint diese Erlaubnis äußerst fragwürdig.

[599] Im Vergleich zu Art 8 GRC ist dieser allerdings nur von „*programmatischer Natur*"; vgl *Abplanalp/Zopf* in *Forgó* (Hrsg), Grundriss Datenschutzrecht (2019) 27.

zwischen der EU und ihren MS im Datenschutzrecht vor (Art 16 Abs 2 AEUV).[600] Art 16 AEUV gilt zudem als besondere Ausprägung der allgemeinen Binnenmarktkompetenz für den freien Datenverkehr (Art 114 AEUV),[601] auf welche die KI-VO ebenfalls gestützt wird (vgl auch ErwGr 3 KI-VO).

Des Weiteren bezieht sich die KI-VO öfters auf die entsprechenden Formulierungen in der DSGVO, insb bei der Definition von Begriffen. Bspw versteht sie unter „*personenbezogenen Daten*" solche iSd Art 4 Z 1 DSGVO (Art 3 Z 50 KI-VO). Ebenso wird dem Begriff „*Profiling*" die gleiche Bedeutung zugemessen wie in Art 4 Z 4 DSGVO (Art 3 Z 52 KI-VO). Auch die Begriffe der „*biometrischen Daten*" (Art 3 Z 34 KI-VO iVm Art 4 Z 14 DSGVO) sowie der „*besonderen Kategorien personenbezogener Daten*" (Art 3 Z 37 KI-VO iVm Art 9 Abs 1 DSGVO) übernimmt die KI-VO aus der DSGVO. Dafür kennt nur die KI-VO „*synthetische Daten*" (vgl Art 10 Abs 5 lit a KI-VO, Art 59 Abs 2 lit b KI-VO),[602] die allerdings den „*nicht-personenbezogenen Daten*" iSd der DSGVO zuzuordnen sind (Art 3 Z 51 KI-VO). Eine Verarbeitung synthetischer Daten – insb zum Weitertrainieren der KI oder zur Personalisierung von Werbung – ist grds DSGVO-konform,[603] da diese schließlich nur bei der Verarbeitung personenbezogener Daten anwendbar ist.[604] Anderes gilt wohl, wenn – wie bei einer De-Anonymisierung – der Personenbezug (wieder-)hergestellt werden kann.[605]

Die KI-VO kennt auch sog „*Öffnungsklauseln*", die es den MS erlauben, auch strengere nationale Regeln bzgl KI-Systemen einzuführen (vgl zB Art 2 Abs 11 KI-VO hinsichtlich des Schutzes von Arbeitnehmern). Zur „*Haushaltsausnahme*" (Art 2 Abs 10 KI-VO) siehe bereits oben.[606]

---

600 *Schröder* in *Streinz* (Hrsg), EUV/AEUV[3] (2018) Art 16 Rz 8 ff.

601 *Kingreen* in *Calliess/Ruffert* (Hrsg), EUV/AEUV[6] (2022) Art 16 Rz 5.

602 *Gorzala*, KI-Regulierung für Kreditscoring und Bonitätsbewertung, ÖBA 2022, 735 (739): Synthetische Daten sind künstlich erzeugte Daten, die nicht aus realen Ereignissen stammen, sondern anhand statistischer Informationen und der Strukturen der Originaldaten für bestimmte Zwecke von Algorithmen hergestellt werden.

603 Wimmer 4.4.2023, Was sind eigentlich synthetische Daten? abrufbar unter <https://futurezone.at/b2b/synthetische-daten-datenschutz-dsgvo-ki-kuenstliche-intelligenz/402337650> (7.5.2024).

604 *Helminger*, Datenschutzrechtliche Herausforderungen bei der Verwendung von Trainingsdaten, EALR 2022, 46 (49 f).

605 *Kaulartz* in *Kaulartz/Braegelmann* (Hrsg) Rechtshandbuch Artificial Intelligence und Machine Learning (2020) Kap 8.9 Rz 22 ff.

606 Vgl Kapitel 3.1 (Vorbemerkungen zur KI-VO).

Eine Parallele besteht ferner in Bezug auf den räumlichen Anwendungsbereich (Art 2 Abs 1 lit c KI-VO), der sich gleichfalls am „*Marktortprinzip*“[607] orientiert (vgl Art 3 Abs 2 DSGVO): Es genügt daher für die Anwendbarkeit der KI-VO, wenn der Anbieter und Betreiber zwar ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, aber der vom KI-System generierte Output – die „*hervorgebrachte Ausgabe*“ (ErwGr 12 KI-VO) – in der EU verwendet wird. Schon die Absicht, den von diesem System erzeugten Output in der Union zu verwenden, ist ausreichend (vgl ErwGr 22 KI-VO).

Zum Schluss sei darauf hingewiesen, dass der „*risikobasierte Ansatz*“, wie er durch die KI-VO verfolgt wird, zumindest tlw[608] an den Ansatz der DSGVO erinnert.[609] Bereits die DSGVO trifft verschiedene Regelungen je nach Sensibilität der zu verarbeitenden personenbezogenen Daten. Sensible Daten (Art 9 DSGVO) unterliegen einem strengeren Regime als „normale“ personenbezogene Daten. Außerdem besteht bspw die Pflicht zur Durchführung einer DSFA (Art 35 DSGVO) nur bei hohem Risiko. Durch eine frühzeitige analytische Auseinandersetzung können die möglichen Auswirkungen auf die Rechte und Freiheiten natürlicher Personen beim Einsatz von KI erkannt werden. Dies kann zu risikoadäquaten und schützenden Maßnahmen führen. Die DSFA stellt somit ein zentrales Instrument dar, um zu prüfen, ob der Einsatz von KI für eine bestimmte Verarbeitungstätigkeit geeignet ist.[610] Bei bestimmten Hochrisiko-KI-Systemen besteht nun zusätzlich die Verpflichtung, eine Grundrechte-Folgenabschätzung durchzuführen (Art 27 Abs 4 KI-VO).[611]

3.8.2 Abgrenzungsschwierigkeiten?

„*Ungelöste Abgrenzungsprobleme*“[612] anzunehmen, erscheint mit Blick auf die inzwischen stark verbesserte Version der KI-VO nicht (mehr) angebracht. Denn die KI-VO lässt die DSGVO

[607] *Engelmann/Brunotte/Lütkens*, Regulierung von Legal Tech durch die KI-Verordnung, RDi 2021, 317 (319).
[608] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 7.
[609] *Martini* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 4 Rz 10, 151: Im Gegensatz zum datenschutzrechtlichen Rahmen bietet die KI-VO den Anwendern weniger Spielraum in Bezug auf den risikobasierten Ansatz. Während es unter der DSGVO den Beteiligten größtenteils überlassen ist, angemessene Vorkehrungen zur Risikoeinschätzung im Umgang mit personenbezogenen Daten zu ergreifen, legt die KI-VO die Verpflichtungen und Vorgaben präziser fest. Sie hat aus den Lektionen, die aus den Schwachstellen der DSGVO gezogen wurden, gelernt und den risikobasierten Ansatz besser umgesetzt.
[610] *Schürmann*, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316 (319).
[611] Vgl Kapitel 3.3 (Verbot des Social Scoring).
[612] *Hilgendorf* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 1 Rz 52: Auf den Entwurf der KI-VO bezugnehmend.

grds unberührt (Art 2 Abs 7 Satz 2 KI-VO) – sogar sektorübergreifend (ErwGr 9 KI-VO) – und bildet grds keine Rechtsgrundlage für die Verarbeitung (sensibler) personenbezogener Daten (ErwGr 63 KI-VO). Insb sollte die KI-VO keine Rechtsgrundlage iSd Art 22 Abs 2 lit b DSGVO hinsichtlich automatisierter Entscheidungen im Einzelfall inkl Profiling bilden (ErwGr 140 KI-VO).

Beide Verordnungen bestehen damit nebeneinander, sodass es prinzipiell zu keiner Kollision der Regelungsbereiche[613] kommt. Im Gegenteil *„gelten die EU-Rechtsvorschriften zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation für die Verarbeitung personenbezogener Daten iZm den in der KI-VO festgelegten Rechten und Pflichten*" (Art 2 Abs 7 Satz 1 KI-VO). Das Grundrecht auf Schutz personenbezogener Daten wird insb durch die DSGVO gewahrt (ErwGr 10 KI-VO). Darüber hinaus schützt die ePrivacy-RL die Privatsphäre und vertrauliche Kommunikation. Diese EU-Rechtsakte sollen insb die Grundlage für eine nachhaltige und verantwortungsvolle Datenverarbeitung bilden, selbst wenn die Datensätze eine Mischung aus Daten mit und ohne Personenbezug aufweisen. Wichtig ist auch, dass das Recht auf Privatsphäre und den Schutz personenbezogener Daten während des gesamten Lebenszyklus des KI-Systems sichergestellt sein muss (ErwGr 69 KI-VO).

Die bloße Erfüllung der in der KI-VO festgelegten Anforderungen bedeutet daher nicht automatisch, dass ein (Hochrisiko-)KI-System auch aus datenschutzrechtlicher Sicht verwendet werden darf.[614] Es bedarf einer separaten Prüfung der datenschutzrechtlichen Zulässigkeit.[615] Aus diesen Gründen bleiben ferner die Pflichten der Anbieter und Betreiber von KI-Systemen in ihrer Rolle als (gemeinsame) Verantwortliche und/oder Auftragsverarbeiter unberührt, sofern die Konzeption, Entwicklung oder Nutzung von KI-Systemen die Verarbeitung personenbezogener Daten beinhaltet. Es wird deutlich gemacht, dass betroffene Personen weiterhin alle Rechte und Garantien der DSGVO behalten, einschließlich der Rechte iZm der ausschließlich automatisierten Entscheidungsfindung im Einzelfall und dem Profiling (ErwGr 10 KI-VO).

Im Übrigen berührt die KI-VO nicht die Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, die für die Überwachung der Einhaltung des Datenschutzes zuständig sind (ErwGr

613 *Gless/Janal* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 2 Rz 30.
614 EDSA/EDSB 18.6.2021, Gemeinsame Stellungnahme 5/2021, 2.
615 *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 32.

10, 157 KI-VO). Für datenschutzrechtliche Fragestellungen und Beschwerden iZm KI-Systemen sieht sich daher die österreichische DSB zuständig (vgl auch Art 74 Abs 8 KI-VO und ErwGr 36 KI-VO).[616] Sollte die KI-VO jedoch (ausnahmsweise) die Offenlegung von Daten gegenüber nationalen DSB ausschließen, sollte dies nicht die aktuellen oder zukünftigen Befugnisse dieser Behörden außerhalb des Anwendungsbereichs der KI-VO beeinträchtigen (vgl ErwGr 159 letzter Satz KI-VO). Für Aufsichtsbehörden stellt sich die mitunter die schwierige Frage, wie die Begrenzung der Verarbeitung personenbezogener Daten gemäß der DSGVO mit der Risikohierarchie der KI-VO in Einklang gebracht werden kann.

Abgesehen davon kann das Verhältnis zwischen der KI-VO und der DSGVO immer noch gewisse Unklarheiten in einzelnen Situationen aufwerfen.[617] Obwohl die KI-VO grds nicht die DSGVO berührt und sie eigentlich nicht so verstanden werden sollte, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bildet, betont ErwGr 63 KI-VO gleichzeitig, dass „*in der KI-VO ausdrücklich etwas anderes vorgesehen*" ist. Demgemäß sieht die KI-VO auch zwei Durchbrechungen der DSGVO vor: (i) Art 10 Abs 5 KI-VO bzgl der ausnahmsweisen Zulässigkeit der Verarbeitung sensibler Daten beim Training von Hochrisiko-KI, um Verzerrungen entgegenzuwirken[618] sowie (ii) Art 59 KI-VO bzgl der Weiterverarbeitung von personenbezogenen Daten zur Entwicklung bestimmter KI-Systeme im erheblichen öffentlichen Interesse.[619] Die konkreten Auswirkungen dieser Bestimmungen in der Praxis bleiben mE noch abzuwarten.

Ein weiteres nicht unwesentliches Problem könnte in der rechtskonformen Erfüllung der Transparenzpflichten gegenüber Betroffenen liegen. Es ist nämlich davon auszugehen, dass sich die Informationspflichten der KI-VO mit denen der DSGVO (Art 13 f DSGVO) überscheiden werden, insb wenn Emotionserkennungssysteme und biometrische Kategorisierungssysteme verwendet werden, bei denen typischerweise personenbezogene Daten verarbeitet werden.[620] Die praktische Umsetzung einer koordinierten Erfüllung dieser doppelten Pflicht obliegt abermals den Unternehmen. Es zeigt sich erneut ein Bedarf an Konkretisierung in diesem

[616] DSB, FAQ zum Thema KI und Datenschutz (Stand 25.4.2024), abrufbar unter <https://www.dsb.gv.at/download-links/FAQ-zum-Thema-KI-und-Datenschutz.html> (8.5.2024).
[617] *Hilgendorf* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 1 Rz 50.
[618] Vgl Kapitel 3.7.1 (Training von Hochrisiko-KI).
[619] Vgl Kapitel 3.7.3 (KI-Reallabore & Datenschutz).
[620] *Kumkar* in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur KI (2023) § 6 Rz 54.

Bereich. Zudem muss der genaue Umfang der Informationspflichten noch klarer definiert werden, insb hinsichtlich der Offenlegung der involvierten Systemlogik, der Entscheidungsgrundlagen bzw der Faktoren, die zur Entscheidung geführt haben und der Wahrung von Betriebs- und Geschäftsgeheimnissen.

Schlussendlich wird erkennbar, dass es zahlreiche Berührungspunkte zwischen der KI-VO und der DSGVO gibt, die tlw bereits gelöst sind, tlw aber noch Herausforderungen darstellen. Vor diesem Hintergrund sollten Unternehmen Prozesse entwickeln, die den Anforderungen beider Verordnungen gerecht werden.[621] Es ist mE dafür nicht erforderlich, das Rad gänzlich neu zu erfinden. Oft werden KI-Anbieter und -Betreiber auf bewährte datenschutzrechtliche Instrumente und Erfahrungen zurückgreifen und diese auf KI-Systeme übertragen können. Die Identifizierung potenzieller Risiken, die die Grundrechte – insb das Recht auf Schutz personenbezogener Daten – beeinträchtigen könnten, ist heutzutage in vielen Unternehmen Standard. Erfreulicherweise gibt es zunehmend ein Bewusstsein[622] für die Notwendigkeit, sich datenschutzkonform zu verhalten. Meiner Meinung nach wird man dasselbe bei einer verstärkten KI-Compliance bemerken, wenn auch vielleicht nicht von Anfang an.

4 Zusammenfassung & Stellungnahme

In einer Ära, in der Daten zu einer der wertvollsten Ressourcen geworden sind und Technologien wie KI das Marketing revolutionieren, stehen Unternehmen vor der Herausforderung, sich technischen Neuerungen anzupassen, Innovationen voranzutreiben und gleichzeitig den Datenschutz und ethische Standards zu wahren. Dieser Balanceakt zwischen Fortschritt und Verantwortung erfordert ein tiefgreifendes Verständnis der rechtlichen Rahmenbedingungen, technologischen Entwicklungen und potenziellen Risiken.

Die steigende Bedeutung des Datenschutzrechts spiegelt sich nicht zuletzt in der wachsenden Sensibilität der Verbraucher und den verschärften gesetzlichen Anforderungen wider, welche die EU in den letzten Jahren im Rahmen ihrer Digitalstrategie eingeführt hat. Datenschutzrechtliche Problemstellungen iZm dem Online-Marketing umfassen eine Vielzahl von

[621] *Schürmann/Möller*, Die Zukunft gestalten: KI-VO im Fokus des Datenschutz- und Risikomanagements, DSB 2023, 326 (326).

[622] *Ritzer* in *Ruhmannseder/Lehner/Beukelmann,* Compliance aktuell 15010, Rz 2 (Stand 1.3.2024, rdb.at).

Aspekten, die in letzter Zeit verstärkt Einzug in die gesellschaftliche Debatte finden. Dazu gehören die Verwendung undurchsichtiger Tracking-Methoden wie Cookies zur Sammlung von Daten über das Online-Verhalten von Konsumenten, algorithmenbasierte Profiling- und Scoring-Techniken, umstrittene Pay-or-Okay-Konzepte sowie der Einsatz verbraucherrechtlich fragwürdiger Praktiken wie Deepfakes, Nudging und Dark Patterns. Auch das Training von KI-Modellen erfordert oft den Zugriff auf große Mengen von Daten, einschließlich solcher mit Personenbezug, wobei es sehr häufig zu einem Transfer in Drittstaaten außerhalb der EU ohne angemessene Schutzmaßnahmen kommt. Es wird deutlich, dass Unternehmen zunehmend von Daten abhängig sind und viele der angewendeten Methoden nicht mit den Vorgaben der DSGVO übereinstimmen. Diesbezüglich ist anzuerkennen, dass die EU-Gerichte und andere Institutionen der EU sowie die DSB in jüngerer Zeit vermehrt Entscheidungen fällen, um den übermäßigen Datensammlungspraktiken zur Personalisierung von Werbeinhalten entgegenzuwirken. Obwohl einige grundlegende Urteile noch ausstehen, zeichnet sich eine Tendenz ab, den Grundrechten einer Person auf den Schutz ihrer personenbezogenen Daten und Privatsphäre einen höheren Stellenwert beizumessen. Um eine langfristige Einhaltung der Vorschriften sicherzustellen, ist es daher entscheidend, bereits bei der Entwicklung von Marketingkonzepten datenschutzkonforme Maßnahmen proaktiv zu berücksichtigen.

Während die positiven Auswirkungen von KI-Systemen, einschließlich ihres Beitrags zum „Gemeinwohl“, häufig und gerne hervorgehoben werden, ist es wichtig, sich nicht den bestehenden und va zukünftigen Gefahren und Risiken zu verschließen oder sie allein im Namen des technologischen Wandels hinzunehmen. Obwohl es derzeit noch fraglich ist, ob KI tatsächlich eine Form von „Intelligenz“ darstellt – trotz beeindruckender Fortschritte – ist es schon heute wesentlich zu erkennen, dass sich diese Technologien in einem quasi exponentiellen Tempo – selbst? – weiterentwickeln. Dies eröffnet nicht nur mehr Möglichkeiten für Anwendungen, sondern erhöht auch die Wahrscheinlichkeit, dass sie schädliche Auswirkungen auf die Grundrechte und Freiheiten der Einzelnen haben. Die Entwicklung und der Einsatz von KI stehen vielmehr in einem inhärenten Konflikt zwischen Datennutzung und Datenschutz. Deshalb ist es unerlässlich, abseits ethischer Überlegungen, die spezifischen datenschutzrechtlichen Anforderungen iZm KI besonders zu berücksichtigen. Dies gilt insb in Bezug auf die Grundsätze (Art 5 DSGVO) sowie die Rechtsgrundlagen einer Datenverarbeitung (Art 6 Abs 1 DSGVO bzw

Art 9 Abs 2 DSGVO), um dem Gespenst des „gläsernen Bürgers“ auch im privaten Bereich entgegenzuwirken.

Zweifellos tangiert die Nutzung von KI praktisch alle Datenverarbeitungsgrundsätze. Beginnend mit der potenziellen Missachtung des strengen Zweckbindungsgrundsatzes, va bei der (Weiter-)Verarbeitung zu Trainingszwecken, erfordert der Einsatz von KI-Systemen eine gewissenhafte Auseinandersetzung mit den einschlägigen Vorgaben zur Transparenz, Datenminimierung und Speicherbegrenzung. Unternehmen sind oft in Versuchung, mehr Daten zu sammeln, als es für ihre Marketingzwecke wirklich notwendig ist. Darüber hinaus können es komplexe KI-Algorithmen selbst für die betreffenden Unternehmen schwierig machen, den genauen Prozess der Datenverarbeitung und -analyse nachzuvollziehen, was wiederum die Einhaltung der Informationspflichten der DSGVO erschwert. Zusätzlich müssen Verantwortliche auf die Richtigkeit der zu verarbeitenden Daten achten. Wenn dies nicht der Fall ist, sind sie verpflichtet, die Daten unverzüglich zu löschen oder zu korrigieren. Gerade die evtl Diskriminierung und Voreingenommenheit durch KI aufgrund von unvollständigen oder fehlerhaften Datensätzen, die zu verzerrten Ergebnissen führen und bestimmte Verbrauchergruppen benachteiligen können, kann ernsthafte Auswirkungen auf das Ansehen einer Marke haben. Ferner wird die Glaubwürdigkeit von Unternehmen beeinträchtigt, wenn diese gefälschte Inhalte mittels KI-Programmen erzeugen lassen. Folglich müssen Verantwortliche im Rahmen ihrer Rechenschaftspflicht gem Art 5 Abs 2 DSGVO jederzeit die Einhaltung dieser Grundsätze auch in dieser Hinsicht nachweisen können.

Vielfach mangelt es auch an einer Legitimität der Verarbeitung an sich, indem persönliche Informationen extrapoliert oder Profile erstellt werden, ohne dass die Betroffenen davon wissen oder zustimmen. Weiters ist die Verwendung personenbezogener Daten für Trainingszwecke nicht automatisch durch die ursprüngliche Rechtsgrundlage gedeckt. In solchen Fällen sind Unternehmen entweder erneut auf eine (ausdrückliche) Einwilligung der betroffenen Personen angewiesen oder müssen eine sorgfältige Interessenabwägung durchführen und diese dokumentieren. Allerdings hat dabei das berechtigte Interesse der Unternehmen den idR überwiegenden Interessen der Betroffenen am Schutz ihrer Daten zu weichen. Selbstverständlich müssen auch Datensicherheitsmaßnahmen implementiert werden, um sowohl Cyberangriffe als auch unbefugte Zugriffe innerhalb des Unternehmens selbst auszuschließen.

Eine oftmals unklare datenschutzrechtliche Rollenverteilung sowie intransparente und exzessive Datenerhebungen, wie sie oft beim Scraping vorkommen, machen es Einzelpersonen schwer, die genauen Auswirkungen zu verstehen und ihre Rechte gemäß der DSGVO effektiv durchzusetzen. Besonders problematisch dürfte es ua für Unternehmen sein, den Begehren zur Auskunftserteilung, Berichtigung oder Löschung möglicherweise nicht ausreichend oder sogar überhaupt nicht nachzukommen. Es bleibt fraglich, wie das bereits anerkannte „Recht auf Vergessenwerden" im Zeitalter von KI umgesetzt werden soll. Dies stellt Unternehmen bereits im herkömmlichen Internet vor erhebliche Schwierigkeiten und die Herausforderungen könnten sich mit dem Einzug von KI noch weiter verschärfen. Aktuell mag eine Anonymisierung noch ein wirksames Mittel sein, um einen Personenbezug zu entfernen. Es ist jedoch anzunehmen, dass KI in Zukunft diese Hürde mühelos überwinden wird und aus wenigen Datensätzen Rückschlüsse auf Individuen ziehen kann. In diesem Bereich liegt die Herausforderung aber mehr in der Technologie als im Recht, da hierzu bereits jetzt rechtliche Vorgaben vorhanden sind. Es bedarf daher geeigneter technologischer Maßnahmen, um angemessene Barrieren zu schaffen.

Die Frage, ob die KI-VO als Lösung für aktuelle und zukünftige Probleme betrachtet werden kann, ist meiner Meinung nach differenziert zu beantworten. Grds unterstütze ich den risikobasierten Ansatz, den dieser EU-Rechtsakt verfolgt. Es ist unbestritten, dass die Gratwanderung zwischen einer Überregulierung und einer Vernachlässigung der Auswirkungen von KI-Systemen äußerst diffizil ist. Einerseits müssen die Grundrechte geschützt werden, andererseits darf Europa nicht hinter den beiden globalen Playern USA und China zurückfallen und noch stärker von ihnen (technologisch) abhängig werden.

Demnach werden die gegenwärtigen Herausforderungen meiner Meinung nach durch die KI-VO weitgehend angemessen berücksichtigt. Generell ist es durchaus bemerkenswert zu sehen, dass die EU trotz der üblichen politischen Auseinandersetzungen und des Lobbyeinflusses letztendlich auch GPAI in die KI-VO aufgenommen hat. Es ist zB offensichtlich, dass Chatbots, die ausschließlich für die automatisierte Kommunikation mit Kunden entwickelt wurden, um Fragen zu Produkten oder Dienstleistungen zu beantworten, oder KI-Systeme, die Geschriebenes lediglich besser formulieren sollen, grundrechtlich geschützte Bereiche wenig bis gar

nicht berühren. Gegen solche Systeme spricht auch nichts, außer vielleicht die potenzielle Bedrohung von Arbeitsplätzen. Diese Modelle und Systeme dienen hauptsächlich der Arbeitserleichterung, der Beschleunigung von Arbeitsprozessen und im Endeffekt der Kosteneinsparung. Zudem scheint die EU – im Vergleich zum ursprünglichen Entwurf der KI-VO – eine größere Anzahl von KI-Systemen zumindest als hochriskant einzustufen (zB Profiling-Systeme).

Es gibt hingegen konkrete Versäumnisse im Katalog der verbotenen KI-Praktiken, der mit zahlreichen Ausnahmen und unbestimmten Begriffen versehen wurde. Diese sind zunächst auslegungsbedürftig und bieten Unternehmen daher eine gewisse Flexibilität bei der Anwendung. Insb bei verhaltensmanipulierenden Systemen besteht das Risiko, dass einige Unternehmen die Vorgaben vorerst weniger streng auslegen als andere, was zu langwierigen Rechts-streitigkeiten – ähnlich wie bei der DSGVO – führen könnte, bis Klarheit durch Aufsichtsbehörden und Gerichte geschaffen wird. Auch sonst ist Art 5 KI-VO von zahlreichen Lücken und Rechtsunsicherheiten geprägt. Nicht einzusehen ist überdies, warum für bestimmte Anwendungen, ua Deepfakes, pauschale Transparenz- und Kennzeichnungspflichten vorgesehen wurden. Dies unterstreicht auch die komplizierte Beziehung zwischen Werbung und KI und die Sorgfalt, die Unternehmen aufwenden müssen, um alle Vorschriften – insb Datenschutz-, Verbraucherschutz- und Wettbewerbsrecht – einzuhalten. Hier hätte man ruhigen Gewissens besser unterscheiden können und eindeutig klarstellen müssen, dass täuschende und manipulierende Praktiken absolut verboten sind, wenn sie Verbrauchern Schäden jeglicher Art verursachen. Es wäre wünschenswert, dass die zuständigen EU-Organe und Einrichtungen rasch detaillierte FAQs, Leitlinien und Durchführungs-VO veröffentlichen, um Rechtsanwendern die Grenzen für die Anwendung solcher Systeme aufzuzeigen.

Zenner[623] ist der Ansicht, dass Fragen rund um Werbung und Marketing zu den Bereichen der KI-VO gehören, die von den Verhandlungsführern weit gefasst wurden, um sie zukunftssicher zu machen. Er führte außerdem aus, dass weitere Definitionen in Bereichen, die sich auf den Werberaum auswirken könnten, voraussichtlich eher über Verhaltenskodizes als über Richtlinien eingeführt werden. Solche Informationen werden jedoch wahrscheinlich erst ab 2026 verfügbar sein. Es ist wichtig zu betonen, dass selbst die Wissenschaftler während der

[623] IAPP 12.6.2024, Marketing sits in a gray zone under EU AI Act, abrufbar unter <https://iapp.org/news/a/at-aigg-2024-marketing-sits-in-a-gray-zone-under-eu-ai-act> (21.6.2024).

Verhandlungen uneins darüber waren, ob Wasserzeichen die Lösung für künstlich erzeugte Inhalte darstellen. Zudem wurden Dark Patterns ursprünglich als ein regelungsbedürftiger Anwendungsfall der KI-VO in Betracht gezogen, doch wurde dies wieder verworfen mit der Begründung, dass diese bereits durch den DSA verboten sind. Bisher ist es „*wirklich ein Schuss ins Blaue*" („*really a shot in the dark*") und vielleicht wird man tatsächlich erst am Ende sehen, welche KI-Systeme betroffen sind. Seiner Meinung nach sind nämlich die meisten mit Werbung und Marketing verbundenen Risiken bereits durch bestehende Datenschutz- und Verbraucherschutzgesetze abgedeckt. Dass KI-Marketing-Tools aber nur geringe Risiken für die Verbraucher bergen und dass es selbst im Falle einer automatisierten Entscheidungsfindung unwahrscheinlich ist, dass diese den Schwellenwert von Art 22 DSGVO erreichen und rechtliche oder ähnlich erhebliche Auswirkungen auf den Einzelnen haben,[624] ist meiner Meinung nach jedenfalls unzutreffend. Die in dieser Arbeit dargestellten negativen Folgen von automatisiertem Profiling, Scoring und ausufernder personalisierter Preisbildung sind nur einige Beispiele für Praktiken, die eindeutig Art 22 DSGVO zuwiderlaufen. Im Gegenteil geht auch *Christl*[625] davon aus, dass „*Unternehmen aufgrund der KI die Prozesse hinter der ausgespielten Werbung nicht mehr im Griff haben*".

Das eigentliche Problem bei KI liegt auch in den zukünftigen Herausforderungen, für die die derzeitige Ausgestaltung der KI-VO keine, nur vage oder bloß pro forma Lösungen bietet. Trotz der Bestimmungen in der KI-VO, die eine kontinuierliche Überwachung der KI-Systeme vorsehen, besteht die Gefahr, dass Modelle und Systeme entwickelt werden oder sich selbst weiterentwickeln, die noch stärker in die Grundrechte eingreifen. Dass zB die Grundrechte-Folgenabschätzung nur für bestimmte KI-Systeme gelten soll, ist ein weiteres Zeichen dafür, dass nicht weitsichtig genug gedacht wurde.[626] In absehbarer Zukunft wird KI nicht nur eine unterstützende Rolle bei vielen Tätigkeiten und Entscheidungen einnehmen, sondern diese auch eigenständig durchführen. Die Frage ist, ob Menschen dann noch bereit und in der Lage sind, die Kontrolle über diese Systeme aufrechtzuerhalten und gegebenenfalls die Notbremse zu

[624] FEDMA 6.6.2024, Panel @ IAPP AI Conference: What the AI Act means for marketing, abrufbar unter <https://www.fedma.org/2024/06/06/fedmas-panel-on-ai-act-and-marketing/> (21.6.2024).

[625] *Schulzki-Haddouti/Greis*, Hilft nur ein Verbot personalisierter Werbung? abrufbar unter <https://www.golem.de/news/werbeindustrie-hilft-nur-ein-verbot-personalisierter-werbung-2402-182507-3.html> (21.6.2024).

[626] Dennoch empfiehlt es sich für alle Unternehmen, die KI-basierte Werbesysteme einsetzen, eine solche Abschätzung durchzuführen. Selbst wenn das Ergebnis zeigt, dass das Risiko sehr gering ist, dient dies den Unternehmen als wertvoller Nachweis dafür, dass sie das Marketing-Tool sorgfältig evaluiert haben.

ziehen. Da sich die Abhängigkeit von KI-Systemen in der gesamten Wertschöpfungskette verstärkt, nimmt die Bereitschaft zu allzu strikten Regeln tendenziell jetzt schon ab.

Was aus datenschutzrechtlicher Perspektive bleibt, ist auf die Technologieneutralität der DSGVO zu vertrauen. Der EU-Gesetzgeber hat meiner Ansicht nach den richtigen Schritt unternommen, indem er den rechtmäßigen Einsatz von KI-Systemen an die Einhaltung der DSGVO geknüpft hat. Datenschutzrechtliche Grundsätze sollten daher zukünftig im Lichte von den Gefahren, die von KI ausgehen können, ausgelegt und angewendet werden. Dies steht meiner Meinung nach nicht im Widerspruch zu dem Argument, dass die DSGVO innovationsfeindlich sei. Denn wie kann etwas als „innovativ" angesehen werden, wenn es den fundamentalen Prinzipien der europäischen Wertegemeinschaft wie der Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und der Wahrung der Menschenrechte entgegenwirkt? Das öffentliche Interesse kann und sollte viele Eingriffe rechtfertigen dürfen, aber KI zeigt eine andere Dimension des Gefährdungspotenzials auf, das eine strikte Regulierung erfordert. Es ist essenziell, gerade angesichts der zunehmenden Bedrohungen, die Rechte der Betroffenen zu stärken.

Eine grundlegende Voraussetzung dafür ist Transparenz, und zwar in großem Umfang. Werbetreibende sind verpflichtet, in ihren Datenschutzerklärungen, AVV und VVT klar offenzulegen, wie sie mit KI umgehen. Sie müssen vorsichtig sein, um sicherzustellen, dass sie ethische Standards einhalten, die Privatsphäre und den Datenschutz respektieren und die Integrität ihrer Marketingpraktiken wahren. Andernfalls riskieren sie ernsthafte rechtliche, ethische und finanzielle Konsequenzen. Letztlich sollte es den mündigen Bürgern selbst überlassen sein, zu entscheiden, wie sie mit der Weitergabe ihrer Daten umgehen möchten. Hier liegt das entscheidende Element: die Freiwilligkeit, die beim Einsatz von KI möglicherweise nicht immer gegeben ist.

Literaturverzeichnis

Alon, KI in der Gesundheitstechnologie: Die Datenschutz-Challenge, GRC aktuell 2023, 93.

Alon-Barkat/Busuioc, Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice, Journal of Public Administration Research and Theory 2023, 153.

Ammann/Pohle, KI-Verordnung – Was bisher geschah und jetzt zu tun ist, CB 2024, 137.

Anderl/Ciarnau, Datenschutzrechtliche Herausforderungen bei Generativer KI, ecolex 2023/667, 1078.

Anderl/Tlapak, Neuer Angemessenheitsbeschluss der Kommission für Datentransfers in die USA, ecolex 2023, 796.

Aschauer, (Juristische) Anwendungsmöglichkeiten von Large Language Models, RZ 2024, 15.

Ashkar/Schröder, Das Gesetz über künstliche Intelligenz der Europäischen Union (KI-Verordnung), BB 2024, 771.

Auer-Reinsdorff/Conrad (Hrsg), Handbuch IT- und Datenschutzrecht[3] (2019).

Bachberger-Strolz, Profiling, Targeting, Algorithmen, künstliche Intelligenz – über die Irrwege einer Debatte in der Arbeitsmarktpolitik, WuG 2020, 329.

Baumgartner/Hansch, Onlinewerbung und Real-Time-Bidding, ZD 2020, 435.

Baumüller, Big Data, SWK 23-24/2017, 1064.

Bayer, AI and disinformation, LTZ 2022, 81.

Becker/Feuerstack, Der neue Entwurf des EU-Parlaments für eine KI-Verordnung, MMR 2024, 22.

Benedikt/Pfau, Meta führt im Lichte der EuGH-Entscheidung aus dem Juli 2023 bezahlpflichtiges Abonnement ein, DSB 2024, 6.

Bergauer in *Jahnel* (Hrsg), DSGVO Art 25 (Stand 1.12.2020, rdb.at).

Bergauer, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018/83, 231.

Bichler (Hrsg), Praxishandbuch Marketingrecht (2024).

Bichler, Digital Services Act und Online Marketing, ecolex 2024/120, 222.

Bierbauer, Datenschutzrechtliche Grundsätze bei der Entwicklung Künstlicher Intelligenz, in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2021 (2022) 175.

Binder Grösswang (Hrsg), Digital Law[2] (2020).

Bisset, KI Compliance (Stand 17.1.2024, Lexis Briefings in lexis360.at).

Bisset, KI und Datenschutz (Stand 17.1.2024, Lexis Briefings in lexis360.at).

Bisset/Raabe-Stuppnig, Datenschutz im Telekommunikationsrecht (Stand 22.3.2024, Lexis Briefings in lexis360.at).

Bisset/Schreiber, ChatGPT und Datenschutz, AnwBl 2023/308, 649.

Blasek, Auskunfteiwesen und Kredit-Scoring in unruhigem Fahrwasser, ZD 2022, 433.

Blasek, Die Rolle von Scorewerten bei automatisierten Entscheidungen, ZD 2024, 258.

Blawert, "Transparenz" nach der DSGVO und der KI-VO-E – Ein Rechtsvergleich mit Empfehlungen zur Umsetzung, DSB 2023, 115.

Blümel, Dark Patterns im DSA und DMA: unzulässige digitale Beeinflussung von Entscheidungsprozessen, ecolex 2023/567, 896.

Bogendorfer in *Knyrim* (Hrsg), DatKomm Art 28 (Stand 1.12.2022, rdb.at).

Bogendorfer in *Knyrim* (Hrsg), DatKomm Art 30 (Stand 1.12.2022, rdb.at).

Bomhard, Text und Data Mining auf Grundlage von Webcrawling und Webscraping, InTeR 2023, 174.

Bomhard/Merkle, Europäische KI-Verordnung, RDi 2021, 276.

Bomhard/Siglmüller, AI Act – das Trilogergebnis, RDi 2024, 45.

Borges/Hilber (Hrsg), BeckOK IT-Recht[13.EL] (2023).

Borges/Keil (Hrsg), Rechtshandbuch Big Data (2024).

Böszörmenyi, Google Analytics - kein Risiko, dennoch verboten? ecolex 2023, 164.

Burgstaller/Hermann/Lampesberger, Künstliche Intelligenz (2019).

Busche, Einführung in die Rechtsfragen der künstlichen Intelligenz, JA 2023, 441.

Caldarola/Schrey (Hrsg), Big Data und Recht (2019).

Calliess/Ruffert (Hrsg), EUV/AEUV[6] (2022).

Chibanguza/Kuß/Steege (Hrsg), Künstliche Intelligenz (2022).

Conrad, Künstliche Intelligenz und die DSGVO – Ausgewählte Problemstellungen, KuR 2018, 741.

Dablander, Künstliche Intelligenz und Datenökonomie (Stand 22.3.2024, Lexis Briefings in lexis360.at).

Denga, Die neue transatlantische Datenordnung "Privacy-Framework" und "Privacy Shield II", RIW 2023, 625.

Dieker, Datenschutzrechtliche Zulässigkeit der Trainingsdatensammlung, ZD 2024, 132.

Dix/Seyerlein-Klug, EAID: Exportschlager AI Act – Setzt die EU einen weltweiten Standard für die KI-Regulierung? ZD-Aktuell 2024, 04506 (beck-online).

Dregelies, Der Schutz vor Dark Patterns im DSA, MMR 2023, 243.

Drolz, Mögliche Konsequenzen sowie Prävention eines Cyber-Vorfalls, GRC aktuell 2023, 49.

Dürager, Künstliche Intelligenz – eine besondere Art des Profiling nach der DSGVO, in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2019 (2019) 375.

Ebers (Hrsg), StichwortKommentar Legal Tech (2023).

Ebers/Heinze/Krügel/Steinrötter (Hrsg), Künstliche Intelligenz und Robotik (2020).

Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, 528.

Ebert/Spiecker, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188.

Ehmann/Selmayr (Hrsg), Datenschutz-Grundverordnung[2] (2018).

Eisenberger, ChatGPT: Brauchen wir 2025 noch Jurist:innen? in *Hofmann/Hölscheidt/Mörth/Pirker/Pöschl/Wiederin* (Hrsg), FS Merli (2023) 803.

Eisenberger, Grundrechtliche Herausforderungen durch den Einsatz von KI, in *Österreichischer Juristentag* (Hrsg), Verhandlungen des Einundzwanzigsten Österreichischen Juristentages Wien 2022 I/2 (2024) 144.

Engelmann/Brunotte/Lütkens, Regulierung von Legal Tech durch die KI-Verordnung, RDi 2021, 317.

Etteldorf, EU: Datenschutzbehörden fordern Stellungnahme des EDSA zu Pay-or-Okay-Modellen, ZD-Aktuell 2024, 01558 (beck-online).

Ettig, Warten auf Godot - Noch immer keine Neuregelung für Cookies & Co., KuR 2024 H 4, I.

Feiler/Brandauer, Strenge Regulierung künstlicher Intelligenz bereits in Geltung, AnwBl 2024/122, 258.

Feiler/Forgó, EU-DSGVO und DSG[2] (2022).

Felten/Kofler/Mayrhofer/Perner/Tumpel (Hrsg), Digitale Transformation im Wirtschafts- & Steuerrecht (2019).

Fischer, Die Datenverwertungsgesellschaft, ÖBl 2023/44, 148.

Flamme/Mehlan, Das Phänomen der politischen Online-Werbung im Zeitalter der Digitalisierung, KuR 2022, 571.

Forgó (Hrsg), Grundriss Datenschutzrecht (2019).

Forgó, „In technology, whatever can be done, will be done?" – Gibt es (datenschutz-)rechtliche Grenzen des Einsatzes von KI und, wenn ja, wo verlaufen diese? in *Reindl-Krauskopf/Grafl* (Hrsg), Künstliche Intelligenz – Fluch oder Segen (2020) 91.

Frank/Heine, KI-Einsatz im Betrieb unter der KI-Verordnung, NZA 2023, 1281.

Frank-Woda/Steiner, Datenschutz in der Unternehmenspraxis (2022).

Fülöp, AI Act: Das Ende europäischer Innovation oder Gefahr für den Datenschutz? – eine Relativierung, Dako 2023/42, 82.

Gausling, KI und DS-GVO im Spannungsverhältnis, in *Ballestrem/Bär/Gausling/Hack/von Oelffen* (Hrsg), Künstliche Intelligenz (2020) 11.

Gausling, Künstliche Intelligenz im digitalen Marketing, ZD 2019, 335.

Gausling, Künstliche Intelligenz und DSGVO, DSRITB 2018, 519.

Gerecke (Hrsg), Handbuch Social-Media-Recht (2023).

Gerhartl, Betrachtungen zum AMAS-Algorithmus, ZIIR 2021, 24.

Gerhartl, Der Einsatz künstlicher Intelligenz im Arbeitsrecht, ASoK 2023, 390.

Geringer/Stückler, Daten im Bilanzsteuerrecht, ÖStZ 2020/190, 149.

Geroldinger, Gutachten II: Rechtsdurchsetzung im Verbraucherrecht – prozessuale Aspekte, in *Österreichischer Juristentag* (Hrsg), Verhandlungen des Einundzwanzigsten Österreichischen Juristentages Wien 2022 II/2 (2022) 101.

Gerpott, Bekämpfung von Dark Patterns auf Nutzerschnittstellen mittels neuer EU-Rechtsakte für den digitalen Raum, KuR 2022, 726.

Gersdorf/Paal (Hrsg), BeckOK Informations- und Medienrecht[43.EL] (2023).

Gertz/Aumiller, Legal Tech und Deep Learning – Eine Bestandsaufnahme, LTZ 2022, 30.

Gertz/Martini/Seeliger/Timko, Dark Patterns – eine interdisziplinäre Analyse, LTZ 2023, 3.

Gola/Heckmann (Hrsg), DS-GVO/BDSG[3] (2022).

Golland, Anforderungen an Transfer Impact Assessments bei Datentransfers in unsichere Drittländer, DSB 2021, 229.

Golland, Auf ein Word ..., DSB 2024, 85.

Golland/Kelbch, Kartellrecht vs. Datenschutzrecht: Rechtsgrundlagen für die Datenverarbeitung in sozialen Netzwerken, DSB 2023, 247.

Gorzala, KI-Regulierung für Kreditscoring und Bonitätsbewertung, ÖBA 2022, 735.

Gräfe, Webtracking und Microtargeting als Gefahr für Demokratie und Medien, DSRITB 2018, 27.

Grasser, Herausforderungen einer vertrauenswürdigen Künstlichen Intelligenz, EALR 2020, 14.

Greiner, Guidelines für den Einsatz von Real-Time Bidding, ecolex 2020, 172.

Grünbichler/Salimbeni, Künstliche Intelligenz in Unternehmen: Eine Kategorisierung der Implementierungshürden, GRC aktuell 2023, 127.

Grünzweig, Welche Gesetze braucht künstliche Intelligenz? Die Presse - Recht 2023/359.

Gutjahr/Spiecker/Wilmer, Systemische Privatheit für große, reale Datenverarbeitungssysteme, KuR 2024, 181.

Hacker, A legal framework for AI training data – from first principles to the Artificial Intelligence Act, Law, Innovation and Technology 2021, 257.

Hacker, KI und DMA – Zugang, Transparenz und Fairness für KI-Modelle in der digitalen Wirt schaft, GRUR 2022, 1278.

Hafner-Thomic, Personalisierte Preise im Online-Handel (2024).

Haidinger in *Knyrim* (Hrsg), DatKomm Art 15 (Stand 1.12.2021, rdb.at).

Haidinger in *Knyrim* (Hrsg), DatKomm Art 22 (Stand 1.12.2022, rdb.at).

Hanzl/Pelzmann/Schragl (Hrsg), Handbuch Digitalisierung (2021).

Hartmann, Der persönlichkeitsrechtliche Schutz vor Deepfakes, KuR 2020, 350.

Heiler/Ciarnau, Datenanonymisierung – Der Schlüssel zur Innovation Herausforderungen und Lösungswege in der Praxis, ecolex 2022/114, 166.

Heinzke, Data Act: Auf dem Weg zur europäischen Datenwirtschaft, BB 2023, 201.

Heinzke/Herbers/Kraus, Datenzugangsansprüche nach dem Data Act, BB 2024, 649.

Helminger, Datenschutzrechtliche Herausforderungen bei der Verwendung von Trainingsdaten, EALR 2022, 46.

Herbers/Savary, Der Digital Markets Act kommt, CB 2022, 196.

Herbrich, Personalisierte Online-Werbung: Gemeinsame Verantwortlichkeit für TC-String beim Real-Time-Bidding – Analyse des EuGH-Urteils in der EUGH Aktenzeichen Rs. C-604/22, ZD-Aktuell 2024, 01623 (beck-online).

Hersemeyer/Ludolph, Datenschutzrechtliche Herausforderungen beim Einsatz Künstlicher Intelligenz im Unternehmenskontext, InTeR 2024, 55.

Hessel/Dillschneider, Datenschutzrechtliche Herausforderungen beim Einsatz von Künstlicher Intelligenz, RDi 2023, 458.

Hilgendorf, „Die Schuld ist immer zweifellos“? Offene Fragen bei Tatsachenfeststellungen und Beweis mit Hilfe „intelligenter“ Maschinen, in *Fischer* (Hrsg), Beweis (2019) 229.

Hilgendorf/Roth-Isigkeit (Hrsg), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023).

Hinderks, Die Kennzeichnungspflicht von Deepfakes, ZUM 2022, 110.

Hoeren/Sieber/Holznagel (Hrsg), Handbuch Multimedia-Recht[60.EL] (2023).

Hoffmann, Regulierung der Künstlichen Intelligenz, KuR 2021, 369.

Hoffmann-Riem, Die digitale Transformation als rechtliche Herausforderung, JuS 2023, 617.

Hofmann/Freiling, Personalisierte Preise und das Datenschutzrecht, ZD 2020, 331.

Hofmann/Raue (Hrsg), Digital Services Act (2023).

Hofmeister/Giupponi, The Regulation of the Data Economy, ZfRV 2023/103, 243.

Holzweber/Scharf, Datenmissbrauch im Kartellrecht? Der Fall Facebook, ecolex 2018, 258.

Horak/Spring, Der Facebook-"Like-Button" benötigt die Zustimmung, ÖBl 2019/76, 291.

Hufen, Nudging, JuS 2020, 193.

Humer, Datenzugang nach dem Data Act und dem Digital Markets Act – Game-Changer für Start-ups? ZIIR 2024, 16.

Illibauer in *Knyrim* (Hrsg), DatKomm Art 13 (Stand 1.12.2021, rdb.at).

J. Wendt/D. Wendt, Einigung auf Rechtsrahmen für Künstliche Intelligenz in der EU: AI Act, ZfPC 2024, 86.

Jaeger, Europarecht: Das Neueste auf einen Blick, wbl 2023, 555.

Jahnel in *Jahnel* (Hrsg), DSGVO Art 22 (Stand 1.12.2020, rdb.at).

Jahnel, Datenschutzrechtliche Grenzen des Einsatzes von KI-unterstützten Legal Tech Tools, ÖZW 2023, 117.

Jahnel/Mader/Staudegger (Hrsg), IT-Recht[4] (2020).

Jahnel/Pallwein-Prettner, Datenschutzrecht[3] (2021).

Janal, Haftung und Verantwortung im Entwurf des Digital Services Acts, ZEuP 2021, 227.

Judt/Klausegger, Was ist eigentlich ... Nudging? ÖBA 2020, 416.

Judt/Klausegger, Was ist eigentlich …Marketing 4.0? ÖBA 2022, 677.

Judt/Klausegger, Was sind eigentlich ...Big Data? ÖBA 2019, 432.

Kalbhenn, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, 663.

Kammerl/Kramer/Müller/Potzel/Tischer/Wartberg, Dark Patterns und Digital Nudging in Social Media – wie erschweren Plattformen ein selbstbestimmtes Medienhandeln? BLM-Schriftenreihe 110 (2023).

Kastelitz in *Knyrim* (Hrsg), DatKomm Art 7 (Stand 7.5.2020, rdb.at).

Kaulartz/Braegelmann (Hrsg), Rechtshandbuch Artificial Intelligence und Maschine Learning (2020).

Kerbl, Website und Cookies (Stand 9.4.2023, Lexis Briefings in lexis360.at).

Kern, Automatisierte Entscheidungsfindung nach Art 22 DSGVO bei bloß entscheidungsunterstützenden Systemen wie zB Scoring, ecolex 2024/112, 191.

Kern, Das neue EU-US Data Privacy Framework als Rechtsgrundlage für Datentransfers in die USA, ecolex 2023, 982.

Kinast/Stanonik (Hrsg), Praxishandbuch Datenschutz für KMU (2019).

Klaushofer, Die menschenrechtliche Dimension Künstlicher Intelligenz, ZÖR 2019, 399.

Knapp/Kobler/Richter, Data Cooperatives – Collective Action as an Opportunity for the European Data Economy and a European Data Private Law, InTeR 2023, 7.

Knyrim (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020).

Knyrim/Gerhalter in *Knyrim* (Hrsg), DatKomm Art 49 (Stand 1.10.2023, rdb.at).

Knyrim/Reisinger, Internationaler Datentransfer, RDB Keywords (Stand 13.6.2023, rdb.at).

Kommenda/Schwab, Was tun, wenn sich künstliche Intelligenz unter die Gesellschafter mischt? AR aktuell 2023, 99.

Koreng/Lachenmann (Hrsg), Formularhandbuch Datenschutzrecht[3] (2021).

Kornbeck, Datenschutzrechtsverstöße als kartellrechtlicher Konditionenmissbrauch. Der Fall Facebook vor dem Bundeskartellamt, ÖZK 2022, 245.

Korte, EDSB: Kritik an Einsatz von Microsoft 365 bei der EU-Kommission, ZD-Aktuell 2024, 01629 (beck-online).

Krämer, Die Rechtmäßigkeit der Nutzung von Scorewerten, NJW 2020, 497.

Kraul (Hrsg), Das neue Recht der digitalen Dienste (2023).

Kriwanek/Tuma, Datenschutz: Arbeitsmarktchancen-Assistenzsystem (AMAS) (16.02.2024, LexisNexis Rechtsnews 35079 in lexis360.at).

Kriwanek/Tuma, EuGH: Datenschutz – Datencodierung iZm personalisierter Werbung (14.03. 2024, LexisNexis Rechtsnews 35185 in lexis360.at).

Kriwanek/Tuma, Vorlagefragen zur DSGVO und zu personalisierter Werbung, RdW 2021/504, 632.

Krohn-Grimberghe/Nemeth/Molin, Die Digitalisierung des CFO, CFO aktuell 2016, 21.

Kruesz, Die Regulierung des Einsatzes von Algorithmen in der DS-GVO, im E-DSA und E-DMA: Hält dreifach wirklich besser? jusIT 2021/1, 1.

Kühling/Buchner (Hrsg), DS-GVO/BDSG[4] (2024).

Kumkar/Rapp, Deepfakes, ZfDR 2022, 199.

Lachenmann, EU-Rat stimmt KI-Verordnung zu – neue Pflichten für Unternehmen, MMR-Aktuell 2024, 01359 (beck-online).

Lamprecht, Hektik in der Cyberwelt, CFO aktuell 2023, 111.

Lantwin, Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz? MMR 2019, 574.

Legner, Entscheidungen zum europäischen Kartellrecht im Jahr 2023, GPR 2024, 37.

Leitinger, DSGVO-konforme Datenübermittlung in die USA, ecolex 2021/382, 589.

Lennartz, „Digitale Puppenspieler" – die Nachbildung von Körper und Stimme durch KI, NJW 2023, 3543.

Lenz, Menschliches Gehirn trifft auf Künstliche Intelligenz: Die Implikationen für Veränderungsfähigkeit und betriebliche Transformationsprozesse, in *Harwardt/Niermann/Schmutte/Steuernagel* (Hrsg), Lernen im Zeitalter der Digitalisierung (2023) 161.

Lettl, Das Gesetz über digitale Märkte (Digital Markets Act - DMA), WRP 2022, 1453.

LfDI Baden-Württemberg, Bußgeldverfahren wegen Massenspeicherung von biometrischen Daten aus Gesichtsscan, ZD-Aktuell 2023, 01016 (beck-online).

Linardatos, Auf dem Weg zu einer europäischen KI-Verordnung – ein (kritischer) Blick auf den aktuellen Kommissionsentwurf, GPR 2022, 58.

Linderkamp, Der digitale Preis – eine automatisierte Einzelfallentscheidung? ZD 2020, 506.

Lobinger, (Chat-)GPT in der juristischen Leistungserbringung – Möglichkeiten und Grenzen, LTZ 2023, 187.

Lorenz, Chatbots im praktischen Einsatz: Grundbegriffe, Rechtsfragen und Anwendungsszenarien, KuR 2019, 1.

Luketina/Mathy/Staudingeri/Schütz/Stadlbauer/Kuci, Predictive Analytics in der öffentlichen Verwaltung: Rechtliche und technische Aspekte, aktuelle Anwendungsfälle, Problem stellungen und Möglichkeiten, ZTR 2021, 150.

Malorny, Datenschutz als Grenze KI-basierter Auswahlentscheidungen im Arbeitsrecht, RdA 2022, 170.

Maran, Datenschutzkonformes Tracking zu Werbe- und Marketingzwecken. Das "Pur-Abo-Modell" und "Leistung gegen Daten", CB 2023, 345.

Martini/Drews/Seeliger/Weinzierl, Dark Patterns, ZfDR 2021, 47.

Martini/Kramme/Seeliger, „Nur noch für 30 Minuten verfügbar" – Scarcity- und Countdown-Patterns bei Online-Geschäften auf dem Prüfstand des Rechts, VuR 2022, 123.

Martini/Nink, Wenn Maschinen entscheiden …, NVwZ 2017, 681.

Mayer, Webshop-Recht[2] (2019).

Mayrhofer/Nessler/Bieber/Fister/Homar/Tumpel (Hrsg), ChatGPT, Gemini & Co (2024).

Mertens, OLG Stuttgart: Direktwerbung und Adresshandel können berechtigte Interessen dar stellen, DSB 2024, 104.

Messner/Mosing, ÖDSB: Datenübermittlung durch Implementierung von Google Analytics, ZD 2022, 493.

Moos/Schefzig/Arning (Hrsg), Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap 6 (Stand 1.4.2021, rdb.at).

Müller-Peltzer/Guttmann, "State of the art" Webtracking – aktuelle Entwicklungen, aufsichtsbehördliche und gerichtliche Positionen, DSB 2023, 233.

Müller-Peltzer/Tanczik, Künstliche Intelligenz und Daten, RDi 2023, 452.

Nemec, Digital Services Act und Verbraucherschutz, ecolex 2024/119, 219.

Neufeld, ChatGPT – das Ende der Unschuld, BB 2023 H 7, I.

Nikol/Rost, "Pay or okay" – okay or not okay? Aktuelle Entwicklungen bei den sog. Pur-Modellen, DSB 2023, 167.

Oehler, Predictive Analytics, CFO aktuell 2018, 25.

Paal, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, ZfDR 2024, 129.

Paal/Pauly (Hrsg), DS-GVO/BDSG[3] (2021).

Pfeiffer/Helmke, Die Digitalrechtsakte der EU (DGA, DSA, DMA, KI-VO-E und DA-E) – Teil I, ZD-Aktuell 2023, 01125 (beck-online).

Pieper, Künstliche Intelligenz im Marketing, in *Lucas/Schuster* (Hrsg), Innovatives und digitales Marketing in der Praxis (2023) 221.

Pils, Datenschutz im Marketing[2] (2024).

Podszun (Hrsg), Digital Markets Act (2023).

Podszun, Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, in *Friedl/Burgi* (Hrsg), Wirtschaft und Recht für Mittelstand und Handwerk 8 (2023) 46.

Pohle, Innovativ – und jetzt? CB 2021, 371.

Polley/Konrad, Der Digital Markets Act – Brüssels neues Regulierungskonzept für Digitale Märkte, WuW 2021, 198.

Pollirer, Checkliste datenschutzgerechte Cookie-Banner, Dako 2022/18, 38.

Prange, Datenschutz- und lauterkeitsrechtliche Kernfragen des Einsatzes Künstlicher Intelligenz im Marketing, WRP 2024, 151.

Qasim, Italien: Kein Freifahrtschein für Gesichtserkennungssoftware – Bußgeld iHv 20 Mio. EUR gegen Clearview AI, ZD-Aktuell 2022, 01144 (beck-online).

Raabe/Wagner, Verantwortlicher Einsatz von Big Data, DuD 2016, 434.

Raffling/Schock (Hrsg), Digitale Wirtschaft und Industrie 4.0 (2018).

Raji, Privilegiertes Training von KI-Systemen, DSB 2022, 193.

Reinecke, Datenschatz und Geschäftsmodell-Disruption: Worin liegt das strategische Potential von KI wirklich? LogR 2024, 3.

Riess, ChatGPT und künstliche Intelligenz, AR aktuell 2023, 129.

Rohrleitner, ChatGPT und Mitarbeiter:innen – ein Risiko? Dako 2023/43, 84.

Roßnagel/Nebel/Richter, Was bleibt vom Europäischen Datenschutzrecht? – Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455.

Rostalski/Weiss, Der KI-Verordnungsentwurf der Europäischen Kommission, ZfDR 2021, 329.

Ruhmannseder/Lehner/Beukelmann, Compliance aktuell 15010 (Stand 1.3.2024, rdb.at).

Russel/Norvig, Künstliche Intelligenz[4] (2023).

Säcker (Hrsg), Münchener Kommentar zum Wettbewerbsrecht 1/14 (2023).

Salomon/Trieb, Ermittlung eines Score-Werts kann das Verbot der automatisierten Entscheidung (Art 22 DSGVO) verletzen, ZFR 2024/50, 119.

Schmidt/Hübener (Hrsg), Das neue Recht der digitalen Märkte (2023).

Schmidt/Hübener (Hrsg), New Digital Markets Act (2023).

Schmidt-Kessel/Grimm, Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten, ZfPW 2017, 84.

Schmoll, Rechtmäßigkeit einer Datenverarbeitung; Grundsätze für die Verarbeitung personenbezogener Daten; Verarbeitung sensibler Daten; Einwilligung der betroffenen Person;

Öffentlichmachen sensibler Daten durch die betroffene Person selbst, Jus-Extra EuGH 2021, 20.

Schneeberger, Intelligente Medizinprodukte: Rechtsfragen am Schnittpunkt von DSGVO, MPVO und AI Act, Dako 2024/3, 4.

Schneider, Cookiebot, DSB 2022, 2.

Schneider, Dark Patterns, DSB 2023, 222.

Schröder (Hrsg), Datenschutzrecht für die Praxis[5] (2023).

Schürmann, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316.

Schürmann/Möller, Die Zukunft gestalten: KI-VO im Fokus des Datenschutz- und Risikomanagements, DSB 2023, 326.

Schwamberger, Der Data Act, ecolex 2024/210, 367.

Schwamberger, Zulässigkeit von "Pay or Okay", jusIT 2019/31, 88.

Schwartmann/Hermann/Mühlenbeck, Eine Medienordnung für Intermediäre, MMR 2019, 498.

Schweiger, Google Analytics: Der nicht rechtskräftige Teilbescheid der DSB, DSB 2022, 52.

Sedef/Steiner, Datenschutz – Auftragsverarbeiter (Stand 11.3.2024, Lexis Briefings in lexis360.at).

Sedef/Steiner, Internationaler Datentransfer (Stand 21.3.2024, Lexis Briefings in lexis360.at).

Sedgewick/Wayne, Algorithmen[4] (2014).

Seeauer, Das ‚Koppelungsverbot' bei Zustimmungserklärungen in AGB, in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2018 (2018) 39.

Simitis/Hornung/Spiecker (Hrsg), Datenschutzrecht (2019).

Škorjanc, Künstliche Intelligenz im Finanzsektor) Zusammenfassung der rechtlichen Aspekte und Ausblick auf den neuen europäischen Rechtsrahmen, ÖBA 2023, 427.

Spindler, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E), CR 2021, 361.

Spindler/Schuster (Hrsg), Recht der elektronischen Medien[4] (2019).

Staudegger, Aktuelles aus dem IT-Recht – Daten-Governance-Rechtsakt (DGA), Gesetz über Digitale Märkte (DMA), Gesetz über Digitale Dienste (DSA), jusIT 2023/40.

Steinrötter (Hrsg) Europäische Plattformregulierung (2023).

Steinrötter, Verhältnis von Data Act und DS-GVO, GRUR 2023, 216.

Streinz (Hrsg), EUV/AEUV[3] (2018).

Sydow/Marsch (Hrsg) DS-GVO/BDSG[3] (2022).

Taeger/Gabel (Hrsg), DSGVO/BDSG/TTDSG[4] (2022).

Thiel, „Deepfakes" – Sehen heißt glauben? ZRP 2021, 202.

Thiele, DSB stattet AMS-Algorithmus mit Ablaufdatum aus, ZIIR 2020, 410.

Thiele, DSB: Einwilligung in Tracking- und Marketing-Cookies zulässig, ZIIR 2023, 37.

Thiele, EuGH: Bundeskartellamt darf DSGVO-Verstöße in Wettbewerbsverfahren prüfen, jusIT 2023/88, 200.

Thiele, EuGH: Setzen von Cookies erfordert aktive Einwilligung des Internetnutzers, ZIIR 2019, 440.

Thiele, Vorlageantrag des OGH: Personalisierte Facebook Werbung – Bloße Vertragserfüllung oder Einwilligungsbedürftigkeit? jusIT 2021/90, 241.

Thurner, Bildmanipulation und Persönlichkeitsschutz in Zeiten von „Deepfakes", MR 2019, 155.

Tichy/Leissler/Woller, Cloud Computing (2019).

Valta/Vasel, Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz, ZRP 2021, 142.

Veale/Borgesius, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97.

Vilain, Speech by Zoé Vilain – Digital Rights and Corporate Accountability: Lessons from Clearview AI and ChatGPT, AnwBl 2024/145, 284.

Wagner, „Tausche persönliche Daten gegen Prozente". Datenschutzrechtliche Anforderungen der Datengenerierung zur Durchführung von Werbemaßnahmen mithilfe elektronischer Post („Leadgenerierung"), in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2023 (2024) 363.

Waxnegger, Künstliche Intelligenz und Strafrecht (2024).

Weinzierl, Neue Dark-Patterns-Verbote als Abschied vom homo oeconomicus im EU-Recht, EuZW 2024, 345.

Weiss, Artikelserie ChatGPT im Kanzleialltag nutzen, AnwBl 2024/119, 234.

Wichering, Die Woche im Blick, BB 2023, 2945.

Wiedemann/Conrad/Salemi, Bereitstellung von Daten nach dem Data Act – offene Fragen und verbleibende Probleme, KuR 2024, 157.

Willis, Deception by Design, Harvard Journal of Law & Technology[vol.34] Number 1 Fall 2020, 116.

Wilmer, Rechtsfragen bei ChatGPT & Co., KuR 2023, 233.

Woerlein, Personalisierte Werbung und Tracking bei Facebook und Instagram – Abo-Modell statt Datenschutz? ZD-Aktuell 2023, 01467 (beck-online).

Wolfbauer/Demschik, Datenverarbeitung im Zeitalter des Metaverse, ecolex 2022/348, 512.

Wolff/Brink/von Ungern-Sternberg (Hrsg), BeckOK Datenschutzrecht[47.EL] (2024).

Yeung, 'Hypernudge': Big Data as a mode of regulation by design, Information Communication and Society (2016).

Zankl, KI: Hohes Risiko nur unter menschlicher Aufsicht, Die Presse - Recht 2021/147.

Zuboff, Das Zeitalter des Überwachungskapitalismus (2019).

Entscheidungsverzeichnis

EuGH

EuGH 6.10.2015, C-362/14 (*Schrems I*) ECLI:EU:C:2015:650.

EuGH 19.10.2016, C-582/14 (*Breyer*) ECLI:EU:C:2016:779.

EuGH 10.7.2018, C-25/17 (*Jehovan todistajat*) ECLI:EU:C:2018:551.

EuGH 29.7.2019, C-40/17 (*Fashion ID*) ECLI:EU:C:2019:629.

EuGH 1.10.2019, C-673/17 (*Planet49*) ECLI:EU:C:2019:801.

EuGH 16.7.2020, C-311/18 (*Schrems II*) ECLI:EU:C:2020:559.

EuGH 26.4.2022, C-401/19 (*Polen/EP und Rat*) ECLI:EU:C:2022:297.

EuGH 4.7.2023, C-252/21 (*Meta u.a./BKartA*) ECLI:EU:C:2023:537.

EuGH 7.12.2023, C-634/21 (*SCHUFA Holding AG*) ECLI:EU:C:2023:957.

EuGH 7.3.2024, C-604/22 (*IAB Europe*) ECLI:EU:C:2024:214.

EuGH 27.3.2024, C-639/23 P(R) (*EK/Amazon*) ECLI:EU:C:2024:277.

EuGH laufend, C-446/21 (*Schrems/Facebook*).

EuG

EuG 26.4.2023, T-557/20 (*Single Resolution Board*) ECLI:EU:T:2023:219.

EuG 12.10.2023, T-553/23 R (*Latombe*) ECLI:EU:T:2023:621.

EuG laufend, T-553/23 (*Latombe*).

Schlussanträge

GA *Pikamäe*, SA 16.3.2023, C-634/21 (*SCHUFA Holding AG*) ECLI:EU:C:2023:220.

GA *Rantos*, SA 25.4.2024, C-446/21 (*Schrems/Facebook*) ECLI:EU:C:2024:366.

VwGH

VwGH 14.12.2021, Ro 2021/04/0007.

VwGH 21.12.2023, Ro 2021/04/0010.

OGH

OGH 24.10.2019, 6 Ob 56/19g.

OGH 15.4.2021, 6 Ob 35/21x.

OGH 23.6.2021, 6 Ob 56/21k.

OGH 19.7.2023, 6 Ob 134/23h.

BVwG

BVwG 12.3.2019, W214 2223400-1.

BVwG 18.12.2020, W256 2235360-1.

BVwG 2.9.2022, W214 2230686-1.

BVwG 26.4.2024, W211 2281997-1.

DSB

DSB 30.11.2018, D122.931/0003-DSB/2018.

DSB 5.12.2018, D123.270/0009-DSB/2018.

DSB 16.4.2019, D213.679/0003-DSB/2018.

DSB 20.8.2019, D122.974/0001-DSB/2019.

DSB 16.8.2020, D123.1020 (2020–0-513.605).

DSB 22.12.2021, D155.027 (2021-0.586.257).

DSB 22.4.2022, D155.026 (2022-0.298.191).

DSB 29.3.2023, D124.4574 (2023-0.174.027).

DSB 9.5.2023, D130.703 (2022-0.277.156).

DSB 20.12.2023, D036.500 (2023-0.891.733).

BKartA

BKartA 6.2.2019, B6-22/16.

OLG Düsseldorf

OLG Düsseldorf 24.3.2021, VI-Kart 2/19 (V).

Rechtsaktverzeichnis

EU-Recht

AEUV: Vertrag über die Arbeitsweise der EU (konsolidierte Fassung), ABl 2012/C 326, 47.

Cookie-RL: RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 zur Änderung der RL 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der VO (EG) Nr 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl 2009/L 337, 11.

DA: VO (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der VO (EU) 2017/2394 und der RL (EU) 2020/1828 (Datenverordnung), ABl 2023/Reihe L, 1.

DGA: VO (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30.5.2022 über europäische Daten-Governance und zur Änderung der VO (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl 2022/L 152, 1.

DMA: VO (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der RL (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl 2022/L 265, 1.

DSA: VO (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der RL 2000/31/EG (Gesetz über digitale Dienste), ABl 2022/L 277, 1.

DSGVO: VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), ABl 2016/L 119, 1.

DSM-RL: RL (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17.4.2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmark und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, ABl 2019/L 130, 92.

E-Commerce-RL: RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft,

insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), ABl 2000/ L 178, 1, zuletzt geändert durch VO (EU) 2022/2065, ABl 2022/L 277, 1.

ePrivacy-RL: RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl 2002/L 201, 37, zuletzt geändert durch RL 2009/136/EG, ABl 2009/L 337, 11.

GRC: Charta der Grundrechte der EU, ABl 2016/C 202, 389.

KI-VO: Legislative Entschließung des Europäischen Parlaments vom 13.3.2024 zu dem Vorschlag für eine VO des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA(2024)0138, zuletzt geändert durch Berichtigung des Europäischen Parlaments vom 17.4.2024 des in erster Lesung am 13.3.2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der VO (EU) 2024/ ..... des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der VO (EG) Nr 300/2008, (EU) Nr 167/2013, (EU) Nr 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der RL 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), P9_TA(2024)0138, (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), cor01.

P2B-VO: VO (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.6.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten, ABl 2019/L 186, 57.

UGP-RL: RL 2005/29/EG vom 11.5.2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der RL 84/450/EWG des Rates, der RL 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der VO (EG) Nr 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl 2005/L 149, 22, zuletzt geändert durch RL (EU) 2019/2161, ABl 2019/L 328, 7.

VO (EU) 2018/1725: VO (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23.10.2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien

Datenverkehr und zur Aufhebung der VO (EG) Nr 45/2001 und des Beschlusses Nr 1247/2002/EG, ABl 2018/L 295, 39.

VO (EU) 2024/900: VO (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13.3. 2024 über die Transparenz und das Targeting politischer Werbung, ABl 2024/Reihe L, 1.

Österreichisches Recht

AMSG: Bundesgesetz über das Arbeitsmarktservice, BGBl Nr 313/1994 idF BGBl I Nr 174/2023.

DSFA-V: VO der DSB über Verarbeitungsvorgänge, für die eine DSFA durchzuführen ist, BGBl II Nr 278/2018.

ECG: Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden, BGBl I Nr 152/2001 idF BGBl I Nr 182/2023.

TKG 2021: Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, BGBl I 190/ 2021 idF BGBl I Nr 6/2024.

UrhG: Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte, BGBl Nr 111/1936 idF BGBl I Nr 182/2023.

UWG: Bundesgesetz gegen den unlauteren Wettbewerb 1984, BGBl Nr 448/1984 idF BGBl I Nr 99/2023.

Verzeichnis sonstiger Quellen

Arbeiterkammer Wien, Verlorene Zeit, Verlorenes Geld – Dark Patterns im Alltag von Konsument:innen März 2023, abrufbar unter <https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/Internet/Dark_Patterns.pdf> (19.4.2024).

Art-29-Datenschutzgruppe 22.6.2010, WP 171, Stellungnahme 2/2010 zur verhaltensbezogenen Werbung, abrufbar unter <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_de.pdf> (18.4.2024).

Art-29-Datenschutzgruppe 2.4.2013, WP 203, Stellungnahme 03/2013 zur Zweckbindung, abrufbar unter <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (16.4.2024).

Art-29-Datenschutzgruppe 10.4.2014, WP 216, Stellungnahme 5/2014 zu Anonymisierungstechniken, abrufbar unter <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (18.4.2024).

Art-29-Datenschutzgruppe 6.2.2018, WP 251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, abrufbar unter <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_de> (26.4.2024).

Breyer 15.3.2024, Offener Brief: Europaabgeordnete fordern Meta zur Abschaffung ihres "Pay or okay"-Modells auf, abrufbar unter <https://www.patrick-breyer.de/offener-brief-europaabgeordnete-fordern-meta-zur-abschaffung-ihres-pay-or-okay-modells-auf> sowie <https://www.patrick-breyer.de/wp-content/uploads/2024/03/MEPs-Letter-to-Meta-on-Pay-or-Okay.pdf> (18.4.2024).

BSI, Exkurs: Social Bots und Chatbots, abrufbar unter <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html> (3.5. 2024).

BSI, Generative AI Models - Opportunities and Risks for Industry and Authorities[v1.1], abrufbar unter <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Generative_AI_Models.pdf?__blob=publicationFile&v=4> (19.4.2024).

Conceptboard, Der US Cloud Act: Die Bedrohung des europäischen Datenschutzes, abrufbar unter <https://conceptboard.com/de/blog/us-cloud-act-europaeischer-datenschutz/> (24.6.2024).

Deutscher Anwaltverein 25.11.2021, Stellungnahme Nr 57/2021, abrufbar unter <https://anwaltverein.de/de/newsroom/sn-57-21-ki-verordnungsvorschlag-der-eu-kommission> (30.4.2024).

DSB, FAQ zum Thema Cookies und Datenschutz (Stand 20.12.2023), abrufbar unter <https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html> (5.4.2024).

DSB, FAQ zum Thema KI und Datenschutz (Stand 25.4.2024), abrufbar unter <https://www.dsb.gv.at/download-links/FAQ-zum-Thema-KI-und-Datenschutz.html> (8.5.2024).

DSB, Fragen und Antworten, Analytics & Cookies, abrufbar unter <https://www.dsb.gv.at/download-links/fragen-und-antworten.html#Analytics&Cookies> (5.4.2024).

DSK 3.4.2019, Hambacher Erklärung zur Künstlichen Intelligenz, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf> (20.4.2024).

DSK 20.12.2021, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf> (20.4.2024).

DSK 22.3.2023, Bewertung von Pur-Abo-Modellen auf Websites, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf> (7.4.2024).

DSK 6.5.2024, Orientierungshilfe Künstliche Intelligenz und Datenschutz, abrufbar unter <https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf> (8.5.2024).

ECAT, About ECAT, abrufbar unter <https://algorithmic-transparency.ec.europa.eu/about_en> (22.4.2024).

EDSA 8.10.2019, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gem Art 6 Abs 1 lit b DSGVO iZm der Erbringung von Online-Diensten für betroffene Personen$^{v2.0}$, abrufbar unter <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_ guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf> (27.4.2024).

EDSA 4.5.2020, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679[v1.1], abrufbar unter <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf> (9. 5.2024).

EDSA 13.4.2021, Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien[v2.0], abrufbar unter <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_de> (9.5.2024).

EDSA 20.5.2022, Data protection issues arising in connection with the use of Artificial Intelligence, abrufbar unter <https://www.edpb.europa.eu/news/national-news/2022/data-protection-issues-arising-connection-use-artificial-intelligence_de> (11.4.2024).

EDSA 14.2.2023, Leitlinien 03/2022 zu irreführenden Gestaltungsmustern in Schnittstellen von Social-Media-Plattformen: Wie man sie erkennt und vermeidet[v2.0], abrufbar unter <https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf> (9.5.2024).

EDSA 17.4.2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, abrufbar unter <https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf> (18.4.2024).

EDSB 8.3.2024, EDPS Investigation into use of Microsoft 365 by the European Commission, Case 2021-0518, abrufbar unter <https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf> (12.4.2024).

EDSB 11.3.2024, European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies, EDPS/2024/05, abrufbar unter <https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf > (12.4.2024).

Eisenberger 18.4.2024, KI regulieren: Tun wir das Richtige? abrufbar unter <https://rudolphina.univie.ac.at/ki-regulieren-tun-wir-das-richtige> (30.4.2024).

EK 6.5.2003, Empfehlung betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl 2003/L 124, 36.

EK 29.12.2021, Leitlinien zur Auslegung und Anwendung der RL 2005/29/EG, ABl 2021/C 526, 1.

EK 24.2.2023, JRC portfolio 15: Trustworthy AI, abrufbar unter <https://joint-research-centre.ec.europa.eu/jrc-science-and-knowledge-activities/trustworthy-artificial-intelligence-ai_en> (22.4.2024).

EK 10.7.2023, Adequacy decision for the EU-US Data Privacy Framework, C(2023) 4745 final, abrufbar unter <https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en> (10.4.2024).

EK 5.9.2023, Ernennungsbeschlüsse, abrufbar unter <https://digital-markets-act.ec.europa.eu/gatekeepers_en> (22.4.2024).

EK 12.12.2023, Künstliche Intelligenz – Fragen und Antworten, abrufbar unter <https://ec.europa.eu/commission/presscorner/api/files/document/print/de/qanda_21_1683/QANDA_21_1683_DE.pdf> (2.5.2024).

EK 23.2.2024, Questions and answers on the Digital Services Act, abrufbar unter <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> (20.4.2024).

EK 14.3.2024, Liste der designierten VLOPs und VLOSEs, abrufbar unter <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (18.4.2024).

EK 25.3.2024, Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act, abrufbar unter <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689> (19.4.2024).

EK, Trustworthy AI, abrufbar unter <https://ai-watch.ec.europa.eu/topics/trustworthy-ai_en> (22.4.2024).

Erläuterungen zur DSFA-V, § 2 Abs 2 Z 2, abrufbar unter <https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html> (27.4.2024).

eTail25, How Cosabella Is Using AI to Boost Sales with Email, abrufbar unter <https://etaileast.wbresearch.com/blog/how-cosabella-uses-ai-to-boost-sales-with-email> (19.4.2024).

EU-Grundrechteagentur, Getting the future right – Artificial Intelligence and Fundamental Rights Report (2020), abrufbar unter <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf> (2.5.2024).

FEDMA 6.6.2024, Panel @ IAPP AI Conference: What the AI Act means for marketing, abrufbar unter <https://www.fedma.org/2024/06/06/fedmas-panel-on-ai-act-and-marketing/> (21.6.2024).

Hochrangige Expertengruppe für Künstliche Intelligenz 8.4.2019, Ethik-Leitlinien für eine vertrauenswürdige KI, abrufbar unter <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (22.4.2024).

IAPP 16.4.2024, Thoughts on behavioral advertising, Meta and privacy, abrufbar unter <https://iapp.org/news/a/thoughts-on-behavioral-advertising-meta-and-privacy> (19.4.2024).

IAPP 17.4.2024, EDPB opinion on legality of pay-or-consent models in EU GDPR context <https://iapp.org/news/a/edpb-opinion-casts-doubt-on-legality-of-pay-or-consent-models-in-eu-gdpr-context> (19.4.2024).

IAPP 12.6.2024, Marketing sits in a gray zone under EU AI Act, abrufbar unter <https://iapp.org/news/a/at-aigg-2024-marketing-sits-in-a-gray-zone-under-eu-ai-act> (21.6.2024).

Isler, KI-Gestützte Entscheidungsfindung: Wie Geschäftsführer von Künstlicher Intelligenz profitieren können, abrufbar unter <https://www.hagel-it.de/it-insights/ki-gestuetzte-entscheidungsfindung-wie-geschaeftsfuehrer-von-kuenstlicher-intelligenz-profitieren-koennen.html> (2.5.2024).

Kastelitz, FISA 702: USA Cloud-Überwachung wurde verlängert, abrufbar unter <https://researchinstitute.at/fisa-cloud-ueberwachung-vor-der-verlaengerung/> (24.6.2024).

Machnik/Gross 16.3.2022, Die dunkle Seite von Digitalem Nudging, abrufbar unter <https://www.uibk.ac.at/ibf/blog-wirtschaft-und-verantwortung/posts/die-dunkle-seite-von-digitalem-nudging.html> (19.4.2024).

Meßmer/Sängerlaub/Schulz, „Quelle: Internet“? Digitale Nachrichten- und Informationskompetenzen der deutschen Bevölkerung im Test, Studie März 2021, abrufbar unter <https://www.stiftung-nv.de/sites/default/files/studie_quelleinternet.pdf> (3.5.2024).

Ministerkomitee des Europarats 15.3.2024, CM(2024)52-prov1, abrufbar unter <https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411> (30.4.2024).

Norwegische DSB 4.6.2024, Meta vil benytte brukernes bilder og innlegg til å utvikle KI, abrufbar unter <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/meta-vil-bruke-brukernes-bilder-og-innlegg-til-a-utvikle-ki/> (21.6.2024).

Noyb 13.8.2021, News Sites: Readers need to "buy back" their own data at an exorbitant price?! abrufbar unter <https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price> (6.4.2024).

Noyb 11.4.2023, "Pay or Okay" – the beginning of the end? abrufbar unter <https://noyb.eu/en/pay-or-okay-beginning-end> (6.4.2024).

Noyb 10.7.2023, European Commission gives EU-US data transfers third round at CJEU, abrufbar unter <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> (5.4.2024).

Noyb 7.12.2023, EuGH weist Kreditauskunftei SCHUFA in die Schranken, abrufbar unter <https://noyb.eu/de/cjeu-landmark-rulings-credit-ranking-and-review-dpas> (28.4.2024).

Noyb 16.2.2024, 28 NGOs fordern EU-Behörden zur Ablehnung von „Pay or Okay“ bei Meta auf, abrufbar unter <https://noyb.eu/de/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta> sowie <https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf> (18.4.2024).

Noyb 17.4.2024, EDSA-Stellungnahme: Meta darf sich nicht auf "Pay or Okay" berufen, abrufbar unter <https://noyb.eu/de/statement-edpb-pay-or-okay-opinion> (18.4.2024).

Noyb 29.4.2024, ChatGPT provides false information about people, and OpenAI can’t correct it, abrufbar unter <https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it> (29.4.2024).

Noyb 6.6.2024, noyb fordert 11 Behörden auf, Metas Missbrauch persönlicher Daten für KI zu stoppen, abrufbar unter <https://noyb.eu/de/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai> (21.6.2024).

Noyb 14.6.2024, (Vorläufiger) noyb-Sieg: Meta stoppt KI-Pläne in der EU, abrufbar unter <https://noyb.eu/de/preliminary-noyb-win-meta-stops-ai-plans-eu> (21.6.2024).

OECD 5.10.2015, Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report (2015), abrufbar unter <https://www.oecd.org/ctp/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report-9789264241046-en.htm> (9.5.2024).

OECD 3.5.2024, Principles for trustworthy AI, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, abrufbar unter <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (9.5.2024).

OECD, Catalogue of Tools & Metrics for Trustworthy AI, abrufbar unter <https://oecd.ai/en/catalogue/overview> (25.4.2024).

OpenAI 29.3.2024, Navigating the Challenges and Opportunities of Synthetic Voices, abrufbar unter <https://openai.com/blog/navigating-the-challenges-and-opportunities-of-synthetic-voices> (12.4.2024).

OpenAI Business Terms (Stand 14.11.2023), abrufbar unter <https://openai.com/policies/business-terms> (18.4.2024).

OpenAI ChatGPT Geschäftsmodelle, abrufbar unter <https://openai.com/chatgpt/pricing> (10.4.2024).

OpenAI Data Controls FAQ, abrufbar unter <https://help.openai.com/en/articles/7730893-data-controls-faq> (12.4.2024).

OpenAI Enterprise Privacy (Stand 10.1.2024), abrufbar unter <https://openai.com/enterprise-privacy> (18.4.2024).

OpenAI General FAQ, How ChatGPT and our language models are developed, abrufbar unter <https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed> (12.4.2024).

OpenAI GPTs Data Privacy FAQs, abrufbar unter <https://help.openai.com/en/articles/8554402-gpts-data-privacy-faqs> (13.4.2024).

OpenAI Nutzungsbedingungen für Europa (Stand 14.11.2023), abrufbar unter <https://openai.com/de/policies/eu-terms-of-use> (11.4.2024).

OpenAI Policies, abrufbar unter <https://openai.com/policies> (10.4.2024).

OpenAI Policy FAQ, How your data is used to improve model performance, abrufbar unter <https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance> (12.4.2024).

OpenAI Privacy Policy (Stand 15.12.2023), abrufbar unter <https://openai.com/de/policies/eu-privacy-policy> (10.4.2024).

Parlamentarische Versammlung des Europarats 18.4.2024, Opinion 303 (2024), abrufbar unter <https://pace.coe.int/en/files/33517> (30.4.2024).

Rat 11.3.2024, EU führt neue Vorschriften über Transparenz und Targeting politischer Werbung ein, abrufbar unter <https://www.consilium.europa.eu/de/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising> (5.5.2024).

Reuters 24.5.2024, EU data protection board says ChatGPT still not meeting data accuracy standards, abrufbar unter <https://www.reuters.com/technology/eu-data-protection-

board-says-chatgpt-still-not-meeting-data-accuracy-standards-2024-05-24/> (21.6.2024).

Rocher/Hendrickx/de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, nature communications (2019), abrufbar unter <https://www.nature.com/articles/s41467-019-10933-3> (11.4. 2024)

RTR 23.4.2024, Zusammenarbeit im Zeichen des DSA: Datenschutzbehörde, KommAustria und RTR-GmbH definieren Kooperation, abrufbar unter <https://www.rtr.at/medien/presse/pressemitteilungen/Presseinformationen_2024/PI04232024RTRM_MoU_DSB_KOA_RTR.html> (25.4.2024).

RTR, Servicestelle für Künstliche Intelligenz, abrufbar unter <https://www.rtr.at/rtr/service/ki-servicestelle/ki-servicestelle.de.html> (13.4.2024).

Schmidl/Gerhalter, Leitfaden zur Verordnung (EU) 2016/679 (Stand September 2022), abrufbar unter <https://www.dsb.gv.at/download-links/dokumente.html> (26.4.2024).

Schulzki-Haddouti/Greis, Hilft nur ein Verbot personalisierter Werbung? abrufbar unter <https://www.golem.de/news/werbeindustrie-hilft-nur-ein-verbot-personalisierter-werbung-2402-182507-3.html> (21.6.2024).

Sommer 22.3.2024, Europaratskommission verabschiedet zahnlose KI-Konvention, abrufbar unter <https://www.digitale-gesellschaft.ch/2024/03/22/europaratskommission-verabschiedet-zahnlose-ki-konvention-wieviel-transparenz-vertraegt-geopolitik> (30.4.2024).

Stenner, Emotionale KI: Berechnete Gefühle, abrufbar unter <https://netzpolitik.org/2021/emotionale-ki-berechnete-gefuehle> (2.5.2024).

TheVerge 12.4.2024, House votes to reauthorize FISA, without the warrant requirement amendment, abrufbar unter <https://www.theverge.com/2024/4/12/24128600/fisa-section-702-house-votes-to-reauthorize-warrant-requirement> (18.4.2024).

U.S. Department of Commerce, Data Privacy Framework List, abrufbar unter <https://www.dataprivacyframework.gov/list> (10.4.2024).

Uuk 18.1.2022, Future of Life Institute: Manipulation and the AI Act, 2, abrufbar unter <https://futureoflife.org/wp-content/uploads/2022/08/FLI-Manipulation_AI_Act.pdf> (5.5.2024).

Vasella 12.3.2024, EuGH i.S. IAB Europe: weite Auslegung des Begriffs des Personendatums: Verbindung aufgrund des Zwecks reicht; gemeinsame Verantwortung von IAB mit den

Mitgliedern, abrufbar unter <https://datenrecht.ch/eugh-i-s-iab-europe-weite-auslegung-des-begriffs-des-personendatums-verbindung-aufgrund-des-zwecks-reicht-gemeinsame-verantwortung-von-iab-mit-den-mitgliedern> (10.4.2023).

Wendehorst 14.12.2021, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective, abrufbar unter <https://www.sozialministerium.at/Themen/Konsumentenschutz/Konsumentenpolitik.html> (8.5.2024).

Werum, Unbegrenzte Möglichkeiten – Deepfakes im Marketing, abrufbar unter <https://aric-hamburg.de/allgemein/deepfakes-werbung-marketing/?trk=article-ssr-frontend-pulse_little-text-block> (26.4.2024).

Wimmer 4.4.2023, Was sind eigentlich synthetische Daten? abrufbar unter <https://futurezone.at/b2b/synthetische-daten-datenschutz-dsgvo-ki-kuenstliche-intelligenz/402337650> (7.5.2024).